Pflichtmodul Algebra

– Vorlesungsskript –

Algebra

Dietrich Burde

2020

Inhaltsverzeichnis

1 Einleitung

Die Vorlesung *Algebra* ist Bestandteil des Bachelor-Studiengangs in Mathematik der Universität Wien. Es stellt den Kernpunkt der Ausbildung im Bereich der Algebra im Bachelorstudium dar. Aufbauend auf Vorkenntnisse aus linearer Algebra und Zahlentheorie werden die Studierenden mit dem abstrakt-strukturellen Zugang zur Algebra vertraut gemacht. Die Studierenden erhalten eine fundierte Ausbildung auf den zentralen Teilgebieten der Algebra.

Das Wort *Algebra* kommt aus dem Arabischen - al-ğabr - das Zusammenfügen gebrochener Teile, und bezeichnet das Rechnen mit Gleichungen in Unbekannten. Als Begründer der Algebra gilt der Grieche *Diophantos von Alexandria*, der wahrscheinlich zwischen 100 v. Chr. und 350 n. Chr. lebte. Sein 13 Bände umfassendes Werk *Arithmetica* ist das älteste bis heute erhaltene, in dem Gleichungen in Unbekannten verwendet werden. Bei Gleichungen geht es hauptsächlich um Polynomgleichungen wie etwa

$$x^5 - 4x + 2 = 0$$

in einer Unbekannten x. Allerdings kann man auch mehrere Unbekannte betrachten, wie etwa

$$y^2 = x^3 - 36x.$$

Diese Gleichungen sollen in gewissen Zahlbereichen gelöst werden. Das sind oft Körper wie $\mathbb{R}$ oder $\mathbb{C}$. Es können aber auch ganzzahlige Lösungen gemeint sein. Für $\mathbb{Z}$ oder $\mathbb{Q}$ spricht man von *Diophantischen Gleichungen*, und das ist ein Zweig der Zahlentheorie. Sind die Exponenten höchstens 1, spricht man von linearen Gleichungen, oder linearen Gleichungssystemen, die in der linearen Algebra behandelt werden. Lineare und quadratische Gleichungen in einer Variablen sind leicht zu lösen. Interessanter wird es aber schon bei kubischen Gleichungen. Es bedurfte schon einiger Anstrengungen, um auch nur eine Lösung in einem Spezialfall zu finden. Das gelang Tartaglia im Jahr 1535 mit der Gleichung

$$x^3 + ax = b,$$

mit reellen Zahlen $a, b > 0$. Er zeigte, dass

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}} + \sqrt[3]{\frac{b}{2} - \sqrt{\left(\frac{b}{2}\right)^2 + \left(\frac{a}{3}\right)^3}}$$

eine reelle Lösung ist. Cardano konnte 1545 die allgemeine kubische Gleichung $x^3 + ax^2 + bx + c = 0$ auf den obigen Fall $x^3 + px + q = 0$ reduzieren und fand Lösungsformeln, mit

Ferrari auch für Grad 4. Er motivierte damit auch die Einführung komplexen Zahlen.

In der Neuzeit wurde die Theorie der Gleichungen weiter ausgebaut, durch Leonhard Euler, Joseph-Louis Lagrange und insbesondere auch durch Carl Friedrich Gauß , der 1799 den *Fundamentalsatz der Algebra* bewies: jede Polynomgleichung

$$a_n x^n + \cdots a_1 x + a_0 = 0$$

vom Grad $n \geq 1$ besitzt genau n Lösungen in den komplexen Zahlen.
Um 1830 entwickelte Évariste Galois (1811-1832) die Galoistheorie. Diese kann als der Beginn der modernen Algebra verstanden werden. Galois und unabhängig Niels Henrik Abel lösten das lange offene Problem der Lösung algebraischer Gleichungen von höherem als viertem Grad, wobei man unter Lösung damals die Darstellung durch die üblichen Rechenoperationen und Wurzelausdrücke (Radikale genannt) verstand, indem sie zeigten, dass dies ab dem fünften Grad im Allgemeinen nicht mehr möglich ist (Satz von Abel-Ruffini). Von Galois stammen in diesem Zusammenhang die Anfänge der Gruppentheorie, vor allen Dingen Permutationsgruppen, und Körpertheorie, also endliche Körper, auch Galois-Felder genannt, und Körpererweiterungen. Natürlich kamen dann auch viele weitere algebraische Strukturen hinzu, oft motiviert aus der Zahlentheorie oder Geometrie und anderen Bereichen.

Notationen: Mit $\mathbb{N}$ bezeichnen wir die natürlichen Zahlen $0, 1, 2, \ldots$.

2 Gruppen

2.1 Gruppenaxiome

Definition 2.1. Eine Gruppe G ist eine nicht-leere Menge zusammen mit einer binären Operation $(a, b) \mapsto ab$ von $G \times G \to G$, die die folgenden Axiome erfüllt:

(1) *Assoziativität.* Für alle $g, h, k \in G$ gilt

$$(gh)k = g(hk).$$

(2) *Existenz eines neutralen Elements.* Es existiert ein Element $e \in G$ mit

$$eg = g = ge$$

für alle $g \in G$.

(3) *Existenz eines inversen Elements.* Für jedes $g \in G$ existiert ein Element $g^{-1} \in G$ mit

$$gg^{-1} = e = g^{-1}g.$$

Ein $e \in G$ mit $eg = g = ge$ ist automatisch eindeutig, denn für ein zweites solches Element $e' \in G$ hat man $e' = ee' = e$. Ebenso ist das inverse Element eindeutig.

Bemerkung 2.1.1. Man kann in Definition 2.1 die Bedingungen (2) und (3) durch die folgenden schwächeren Bedingungen (2′) bzw. (3′) ersetzen:

(2′) *Existenz eines links-neutralen Elements.* Es existiert ein Element $e \in G$ mit

$$eg = g$$

für alle $g \in G$.

(3′) *Existenz eines links-inversen Elements.* Für jedes $g \in G$ existiert ein Element $g^{-1} \in G$ mit

$$g^{-1}g = e.$$

Lemma 2.1.2. *Sei G eine Gruppe. Dann gelten die* Kürzungsregeln*, d.h., aus $gh = gk$ folgt $h = k$ und aus $hg = kg$ folgt $h = k$. Ist G endlich, so sind die Kürzungsregeln äquivalent zu Axiom* (3).

Beweis. Angenommen es gilt $gh = gk$ für $g, h, k \in G$. Durch Anwendung von (3) erhalten wir

$$h = g^{-1}gh = g^{-1}gk = k.$$

Aus $hg = kg$ folgt ebenso $h = k$. Angenommen G ist endlich und es gelten die Kürzungsregeln. Dann ist die Linksmultiplikation $L_g \colon x \mapsto gx$ für jedes $g \in G$ injektiv. Da G endlich ist, ist L_g dann auch für jedes $g \in G$ surjektiv. Daraus folgt aber Axiom (3). □

Definition 2.2. Eine Gruppe G heißt *abelsch*, falls sie das Kommutativitätsgesetz erfüllt, d.h.,

$$gh = hg$$

für alls $g, h \in G$.

In diesem Fall schreibt man oft $a + b$ für ab, $-a$ für a^{-1} und 0 für das neutrale Element e. Das ist aber nicht immer der Fall. Für einen Körper K hat man zwei abelsche Gruppen, nämlich $(K, +)$ mit der Addition, und auch $(K^\times, \cdot)$, die multiplikative Gruppe der Elemente ungleich Null in K.

Beispiel 2.1.3. *Hier sind weitere Beispiele von Gruppen.*

1. *Die Gruppe $(\mathbb{Z}, +)$ der ganzen Zahlen bezüglich Addition. Diese unendliche abelsche Gruppe wird auch manchmal multiplikativ geschrieben und mit $C_\infty = \{g^n \mid g \in \mathbb{Z}\}$ bezeichnet.*

2. *Die Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$. Sie ist gegeben durch die Restklassen*

$$\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

modulo n. Multiplikativ geschrieben wird sie mit $C_n = \{e, g, g^2, \ldots, g^{n-1}\}$ bezeichnet, wobei der Buchstabe C für "cyclic" steht. Es gilt $g^n = g^0 = e$.

3. *Die Gruppe $GL_n(K)$. Sie besteht aus allen invertierbaren $n \times n$-Matrizen mit Koeffizienten in einem Körper K. Sie heißt die allgemeine lineare Gruppe vom Grad n. Für $n = 1$ ist $GL_1(K) = K^\times$.*

4. *Die Diedergruppe D_n für $n \geq 3$. Sie besteht aus den Isometrien der Ebene, die ein reguläres n-Eck fixieren, wobei die Operation die Komposition von Isometrien ist. Die Gruppe D_n hat $2n$ Elemente und ist durch*

$$D_n = \{e, r, r^2, \ldots, r^{n-1}, s, rs, r^2s, \ldots r^{n-1}s\}$$

gegeben. Dabei ist r eine Drehung um den Winkel $\frac{2\pi}{n}$, und s eine Spiegelung, so dass $srs^{-1} = r^{-1}$ und $s^2 = e$. Die Elemente $s, rs, r^2s, \ldots r^{n-1}s$ sind Spiegelungen und die Elemente $e, r, \ldots, r^{n-1}$ sind Drehungen des n-Ecks mit $r^n = e$.

5. *Die "freie" Gruppe F_2. Diese Gruppe besteht aus allen reduzierten Wörtern in zwei verschiedenen Buchstaben a und b und ihrer Inversen. Zwei Wörter werden verknüpft, indem man sie hintereinander schreibt. Reduziert bedeutet, dass man so weit wie möglich kürzt, also z.B.*

$$ba^{-2}bb^{-1}a^2b = ba^{-2}a^2b = b^2.$$

Das neutrale Element ist das leere *Wort e.*

Definition 2.3. Sei X eine Menge. Dann ist die Menge aller Bijektionen $f\colon X \to X$ eine Gruppe bezüglich der Komposition von Abbildungen. Sie wird mit $\mathrm{Sym}(X)$ bezeichnet.

Für $X = \{1, 2, \ldots, n\}$ ist $\mathrm{Sym}(X)$ die symmetrische Gruppe S_n mit $n!$ Elementen. Die Diedergruppe D_3 besteht aus den Drehungen und Spiegelungen eines regelmäßigen Dreiecks, mit den Ecken $1, 2, 3$ in der Ebene, die das Dreieck in sich überführen. Die Drehungen sind $\mathrm{id}, (123), (132)$, und die Spiegelungen $(12), (13), (23)$. Hier bedeutet (123) zum Beispiel die Bijektion $\pi\colon \{1,2,3\} \to \{1,2,3\}$ mit $\pi(1) = 2$, $\pi(2) = 3$ und $\pi(3) = 1$. Also hat man

$$D_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\} = S_3.$$

Für $n \geq 4$ hat S_n aber mehr Elemente als D_n. Die Komposition von Elementen $\pi_1, \pi_2 \in S_3$ definieren wir durch

$$(\pi_1 \circ \pi_2)(i) = \pi_1(\pi_2(i))$$

für alle $i \in \{1, 2, 3\}$. Für $\pi_1 = (12)$ und $\pi_2 = (23)$ gilt etwa

$$\begin{aligned}(\pi_1 \circ \pi_2)(1) &= \pi_1(1) = 2,\\ (\pi_1 \circ \pi_2)(2) &= \pi_1(3) = 3,\\ (\pi_1 \circ \pi_2)(3) &= \pi_1(2) = 1.\end{aligned}$$

Das bedeutet $(12) \circ (23) = (123)$. Auf diese Weise kann man die Gruppentafel von S_3 bestimmen.

$\circ$	id	(123)	(132)	(23)	(13)	(12)
id	id	(123)	(132)	(23)	(13)	(12)
(123)	(123)	(132)	id	(12)	(23)	(13)
(132)	(132)	id	(123)	(13)	(12)	(23)
(23)	(23)	(13)	(12)	id	(123)	(132)
(13)	(13)	(12)	(23)	(132)	id	(123)
(12)	(12)	(23)	(13)	(123)	(132)	id

Lemma 2.1.4. *Sei S eine nicht-leere Teilmenge einer Gruppe G. Angenommen, die folgenden zwei Eigenschaften gelten:*

(S1) Für alle $a, b \in S$ gilt $ab \in S$.

(S2) Für alle $a \in S$ gilt $a^{-1} \in S$.

Dann ist S mit der Verknüpfung von G eine Gruppe.

Beweis. Wegen (S1) definiert die binäre Operation auf G auch eine binäre Operation auf S, die die Assoziativität vererbt. Nach Voraussetzung enthält S mindestens ein Element a. Für jedes $a \in S$ liegt sein Inverses a^{-1} und das Produkt $e = aa^{-1}$ wegen (S1) und (S2) wieder in S. Daher folgen die Gruppenaxiome für S aus denen für G. □

Definition 2.4. Jede nicht-leere Teilmenge S einer Gruppe G, die (S1) und (S2) erfüllt, heißt *Untergruppe* von G.

Beispiel 2.1.5. 1. *Die "triviale"Gruppe* $\{e\}$ *und die ganze Gruppe* G *sind Untergruppen von* G.

2. *Das* Zentrum *einer Gruppe* G, *definiert durch*

$$Z(G) = \{g \in G \mid gx = xg \; \forall \, x \in G\},$$

ist eine Untergruppe von G.

3. *Der Schnitt beliebig vieler Untergruppen von* G *ist eine Untergruppe von* G.

4. *Die Teilmenge* $n\mathbb{Z}$ *von* $\mathbb{Z}$ *für* $n \in \mathbb{Z}$ *ist eine Untergruppe von* $\mathbb{Z}$.

Lemma 2.1.6. *Sei* X *eine Teilmenge einer Gruppe* G. *Dann gibt es eine kleinste Untergruppe von* G, *die* X *enthält.*

Beweis. Der Schnitt S aller Untergruppen von G, die X enthalten, ist wieder eine Untergruppe von G, die X enthält. Offensichtlich ist sie die kleinste solche Untergruppe. S enthält mit X auch alle endlichen Produkte von Elementen aus X und deren Inverse. Aber die Menge solcher Produkte erfüllt (S1) und (S2) und ist daher eine Untergruppe S' von G, die X enthält. Offensichtlich gilt $S = S'$. □

Definition 2.5. Die kleinste Untergruppe von G, die X enthält, wird mit $\langle X \rangle$ bezeichnet und heißt die *von* X *erzeugte Untergruppe*. Wir sagen, dass X die Gruppe G *erzeugt* falls $G = \langle X \rangle$, d.h., falls jedes Element von G als endliches Produkt von Elementen aus X und deren Inversen geschrieben werden kann.

Wir setzen $\langle \emptyset \rangle = \{e\} = 1$, welches die triviale Gruppe ist. Die Gruppe, die durch eine Rotation r um den Winkel $\frac{2\pi}{n}$ erzeugt wird, ist durch $C_n = \langle r \rangle = \{e, r, r^2, \ldots, r^{n-1}\}$ gegeben.

Definition 2.6. Eine Gruppe G heißt *zyklisch*, falls sie von einem Element erzeugt ist.

Man beachte, dass zyklische Gruppen abelsch sind, da alle Elemente r^k und r^ℓ kommutieren. Insbesondere sind die Gruppen C_n und C_∞ zyklisch. Die Gruppen $GL_n(K)$ sind für $n > 1$ nicht zyklisch, da sie nicht abelsch sind.

2.2 Gruppenhomomorphismen

Definition 2.7. Eine Abbildung $\varphi\colon G \to H$ zwischen zwei Gruppen heißt *Gruppenhomomorphismus*, falls

$$\varphi(gh) = \varphi(g) \cdot \varphi(h)$$

für alle $g, h \in G$. Ein bijektiver Gruppenhomomorphismus heißt *Gruppenisomorphismus*. Dann heißen die Gruppen G und H *isomorph* und wir schreiben $G \cong H$.

Ist e das neutrale Element von G und e' das neutrale Element von H, dann gilt $\varphi(e) = e'$ für jeden Gruppenhomomorphismus $\varphi\colon G \to H$:

$$\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$$

impliziert durch Kürzung mit $\varphi(e)$, dass $e' = \varphi(e)$. Weiterhin gilt $\varphi(g^{-1}) = \varphi(g)^{-1}$ für alle $g \in G$, weil

$$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e) = e'.$$

Das Inverse eines Gruppenisomorphismus ist wieder ein Gruppenisomorphismus.

Beispiel 2.2.1. *Wir geben drei Beispiele von Gruppenhomomorphismen.*

1. *Sei H eine Untergruppe von G. Dann ist die Einbettung $H \hookrightarrow G$ ein Gruppenhomomorphismus.*

2. *Die Abbildung $\varphi\colon \mathbb{Z} \to \mathbb{Z}$, $x \mapsto nx$, für ein $n \in \mathbb{Z}$ ist ein Gruppenhomomorphismus.*

3. *Die Exponentialabbildung* $\exp\colon (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ *ist ein Gruppenisomorphismus.*

Definition 2.8. Eine Gruppenhomomorphismus $\varphi\colon G \to G$ heißt *Endomorphismus*. Ist er bijektiv, so heißt er *Automorphismus*. Die Automorphismen einer Gruppe G bilden eine Gruppe unter Komposition, die mit $\mathrm{Aut}(G)$ bezeichnet wird.

Zum Beispiel ist die Konjugationsabbildung

$$i_g\colon G \to G, x \mapsto gxg^{-1}$$

ein Automorphismus von G. Die Abbildung ist bijektiv, und es gilt

$$i_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = i_g(x)i_g(y)$$

für alle $g, h \in G$. Also ist i_g ein bijektiver Gruppenhomomorphismus, also ein Automorphismus. Er heißt auch *innerer Automorphismus* von G.

Definition 2.9. Die inneren Automorphismen von G bilden eine Untergruppe von $\mathrm{Aut}(G)$, die mit $\mathrm{Inn}(G)$ bezeichnet wird.

Es gilt

$$(gh)x(gh)^{-1} = g(hxh^{-1})g^{-1}$$

für alle $g, h \in G$, was $i_{gh}(x) = (i_g \circ i_h)(x)$ bedeutet. Die Gruppe $\mathrm{Inn}(G)$ ist genau dann trivial, wenn G abelsch ist.

Definition 2.10. Sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Der *Kern* von φ ist durch

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = e_H\},$$

gegeben und das *Bild* von φ ist durch

$$\mathrm{im}(\varphi) = \{\varphi(g) \mid g \in G\}.$$

gegeben.

Es ist leicht zu sehen, dass $\ker(\varphi)$ eine Untergruppe von G ist, und $\mathrm{im}(\varphi)$ eine Untergruppe von H. Weiterhin ist φ genau dann injektiv, wenn $\ker(\varphi)$ trivial ist.

Wir wollen noch eine Anwendung von Gruppenhomomorphismen geben, nämlich den Satz von Cayley.

Satz 2.2.2 (Cayley)**.** *Für jede Gruppe G gibt es einen injektiven Gruppenhomomorphismus $L\colon G \hookrightarrow \mathrm{Sym}(G)$. Insbesondere ist jede endliche Gruppe der Ordnung n isomorph zu einer Untergruppe der S_n.*

Beweis. Man betrachte die Abbildung $L\colon G \to \mathrm{Sym}(G)$, die durch $g \mapsto L_g$ gegeben ist. Wir haben

$$(L_a \circ L_b)(x) = L_{ab}(x)$$

für alle $a, b, x \in G$, und $L_a \in \mathrm{Sym}(G)$ für alle $a \in G$, da jede Abbildung L_a bijektiv ist. In der Tat, $L_e = \mathrm{id}$ und

$$L_a \circ L_{a^{-1}} = \mathrm{id} = L_{a^{-1}} \circ L_a.$$

Also ist L ein Gruppenhomomorphismus. Er ist injektiv, weil die Kürzungsregeln in G gelten; siehe Lemma 2.1.2. □

2.3 Nebenklassen und Faktorgruppen

Sei S eine Teilmenge einer Gruppe G. Definiere Mengen

$$aS = \{as \mid s \in S\},\ Sa = \{sa \mid s \in S\}.$$

Definition 2.11. Sei G eine Gruppe und H eine Untergruppe von G. Die Mengen der Form aH heißen *Linksnebenklassen* von H, und die Mengen der Form Ha heißen *Rechtsnebenklassen* von H.

Wegen $e \in H$ gilt $aH = H$ genau dann wenn $a \in H$.

Satz 2.3.1. *Sei H eine Untergruppe von G.*

(a) *Ein Element $a \in G$ liegt in einer Linksnebenklasse C von H genau dann wenn $C = aH$.*

(b) *Zwei Nebenklassen sind entweder gleich oder disjunkt.*

(c) *Es gilt $aH = bH$ genau dann wenn $a^{-1}b \in H$.*

(d) *Je zwei Nebenklassen haben die gleiche Kardinalität.*

Beweis. (a): Falls $C = aH$ gilt, haben wir $a \in aH$. Umgekehrt, wenn a in der Linksnebenklasse bH liegt, dann folgt $a = bh$ für ein $h \in H$, und

$$aH = bhH = bH.$$

(b): Angenommen, zwei Nebenklassen C und C' sind nicht disjunkt. Dann gibt es ein a in C und in C', so dass $C = aH = C'$ wegen (a).

(c): Falls $a^{-1}b \in H$, dann folgt $H = a^{-1}bH$ und $aH = aa^{-1}bH = bH$. Umgekehrt, falls $aH = bH$ gilt, dann hat man $H = a^{-1}bH$ und $a^{-1}b \in H$.

(d): The Abbildung $L_{ba^{-1}}\colon aH \to bH$, gegeben durch $ah \mapsto bh$ ist eine Bijektion. □

Definition 2.12. Sei H eine Untergruppe von G. Der *Index* $(G : H)$ von H in G ist die Kardinalität der Menge $\{aH \mid a \in G\}$, d.h., die Anzahl der Linksnebenklassen von H in G.

Für die triviale Untergruppe $H = 1$ gilt $(G : 1) = |G|$. Das ist die *Ordnung* von G, d.h., die Anzahl der Elemente in G. Wir haben

$$G = \bigcup_{a \in G} aH.$$

Da je zwei Nebenklassen gleich oder disjunkt sind, bilden sie eine Partition von G.

Theorem 2.3.2 (Lagrange)**.** *Sei G eine endliche Gruppe, und H eine Untergruppe. Dann gilt*

$$(G : 1) = (G : H)(H : 1).$$

Insbesondere teilt die Ordung einer Untergruppe die Ordnung von G.

Beweis. Die Linksnebenklassen von H in G bilden eine Partition von G. Es gibt $(G : H)$ Nebenklassen, und jede hat $(H : 1)$ Elemente. □

Definition 2.13. Die Ordnung eines Gruppenelements $g \in G$ ist definiert als die Ordnung der zyklischen Untergruppe, die durch g erzeugt wird, d.h., $\mathrm{ord}(g) = |\langle g \rangle|$.

Die Abbildung $\psi \colon \mathbb{Z} \to \langle g \rangle$, $k \mapsto g^k$ ist ein surjektiver Gruppenhomomorphismus mit $\langle g \rangle \cong \mathbb{Z}$ für $\mathrm{ord}(g) = \infty$ und $\langle g \rangle \cong \mathbb{Z}/m\mathbb{Z}$ für $\mathrm{ord}(g) = m$, siehe Beispiel 2.3.16. Ist $\mathrm{ord}(g) = m \in \mathbb{N}$, so folgt aus diesem Isomorphismus

$$g^k = e \Leftrightarrow k \in m\mathbb{Z}.$$

Insbesondere ist die Ordnung von g ist auch die kleinste positive Zahl $k \geq 1$ mit $g^k = e$. Existiert keine solche Zahl, so hat man $\mathrm{ord}(g) = \infty$.

Korollar 2.3.3. *Die Ordnung von g teilt die Ordnung von G für jedes $g \in G$, und es gilt*

$$g^{|G|} = e.$$

Beweis. Man wende Lagrange für die Untergruppe $H = \langle g \rangle$ an und benutze $(H : 1) = \mathrm{ord}(g)$. Aus $\mathrm{ord}(g) \mid \mathrm{ord}(G)$ folgt $\mathrm{ord}(G) \in \mathrm{ord}(g)\mathbb{Z}$, und daher $g^{\mathrm{ord}(G)} = e$. □

Bemerkung 2.3.4. Für die Gruppe $U(n) = (\mathbb{Z}/n\mathbb{Z})^\times$ der invertierbaren Elemente in $\mathbb{Z}/n\mathbb{Z}$ bedeutet $a^{|G|} = e$ auch $a^{\varphi(n)} = 1$, wegen $|U(n)| = \varphi(n)$. Für $n = p$ Primzahl ist das der "kleine Fermat": $a^{p-1} \equiv 1 \bmod p$ für $p \nmid a$.

Korollar 2.3.5. *Jede Gruppe von Primzahlordnung p ist isomorph zu der zyklischen Gruppe C_p.*

Beweis. Sei G eine Gruppe der Ordung p. Dann hat jedes Element die ordung 1 oder p, weil das die einzigen positiven Teiler von p sind. Da G nicht-trivial ist, gibt es ein Element $g \in G$ der Ordnung p. Sei $H = \langle g \rangle \subseteq G$ die zyklische Untergruppe von G, die durch g erzeugt wird. Dann ist $|H| = p$ und $H = G = \{e, g, g^2, \ldots g^{p-1}\}$. □

Zu je zwei Gruppen G und H kann man das *direkte Produkt* $G \times H$ bilden. Es ist das kartesische Produkt von G und H mit der Komposition $(g,h)(g',h') = (gg',hh')$. Diese erfüllt alle Gruppenaxiome. Eine endliche Gruppe G mit $\mathrm{ord}(G) = n$ ist zyklisch genau dann, wenn sie ein Element der Ordnung n hat. Man beachte, dass das direkte Produkt $C_n \times C_n$ die Ordung n^2 hat, aber kein Element der Ordung n^2 für $n \geq 2$. Also ist sie nicht zyklisch. Allerdings gilt nun der folgende Satz.

Satz 2.3.6. *Jede Untergruppe einer zyklischen Gruppe ist zyklisch.*

Beweis. Sei G eine zyklische Gruppe mit Erzeuger g. Für eine Untergruppe $H \subseteq G$ werden wir $H = \langle g^n \rangle$ für ein $n \in \mathbb{N}$ zeigen. Also ist H zyklisch. Die triviale Gruppe ist offenbar von dieser Form. Also können wir annehmen, dass H nicht-trivial ist. Sei n die kleinste positive ganze Zahl mit $g^n \in H$. Ein solches n muss existieren, da H nicht-trivial ist, und somit irgendeine Potenz von g enthalten muss. Wir behaupten, dass jedes $h \in H$ eine Potenz von g^n ist. Wir wissen, dass $h = g^m$ für ein $m \in \mathbb{Z}$. Mit dem Euklidischen Algorithmus in $\mathbb{Z}$ erhalten wir $m = qn + r$ für ganze Zahlen q und r mit $0 \leq r < n$. Also ist

$$h = g^m = (g^n)^q g^r,$$

und $g^r = (g^n)^{-q} h$. Wegen $g^n \in H$ zeigt das $g^r \in H$. Da n aber minimnal war, impliziert $0 \leq r < n$ nun $r = 0$. Also gilt $n \mid m$ und $h = g^m \in \langle g^n \rangle$. das zeigt $H = \langle g^n \rangle$. □

Definition 2.14. Eine Untergruppe N von G heißt *normal* oder *Normalteiler*, falls $gN = Ng$ für alle $g \in G$. Wir schreiben $N \triangleleft G$.

Offenbar ist eine Untergruppe N von G genau dann ein Normalteiler, falls $gNg^{-1} = N$ für alle $g \in G$. In einer abelschen Gruppe ist jede Untergruppe ein Normalteiler. In nicht-abelschen Gruppen muss nicht jede Untergruppe ein Normalteiler sein.

Beispiel 2.3.7. *Sei* $G = GL_2(\mathbb{Z}) = \{A \in M_2(\mathbb{Z}) \mid \det(A) = \pm 1\}$ *und* $N = \{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \mid n \in \mathbb{Z}\}$. *Dann ist* G *eine Gruppe, und* N *eine Untergruppe von* G*, die nicht normal ist.*

Für $g = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in G$ haben wir

$$g \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} g^{-1} = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \notin N.$$

Lemma 2.3.8. *Der Kern eines Gruppenhomomorphismus* $\varphi\colon G \to H$ *ist stets ein Normalteiler von* G*.*

Beweis. Sei $N = \ker(\varphi)$. Es genügt, $aNa^{-1} \subseteq N$ für alle $a \in G$ zu zeigen, da daraus auch $a^{-1}Na \subseteq N$ folgt. Das kann man umschreiben als $aN \subseteq Na$ und $Na \subseteq aN$, was $aN = Na$ für alle $a \in G$ bedeutet.
Sei also $x \in N$, d.h., $\varphi(x) = e_H$. Dann ist

$$\begin{aligned} \varphi(axa^{-1}) &= \varphi(a)\varphi(x)\varphi(a)^{-1} \\ &= \varphi(a)e_H\varphi(a)^{-1} \\ &= e_H. \end{aligned}$$

□

Beispiel 2.3.9. *Der Kern des Gruppenhomomorphismus* $\det\colon GL_n(K) \to K^\times$ *ist ein Normalteiler in* $GL_n(K)$*, der durch*

$$SL_n(K) = \{A \in GL_n(K) \mid \det(A) = 1\}$$

gegeben ist.

Das Argument kann man auch für $GL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) \mid \det(A) = \pm 1\}$ rechtfertigen, d.h.,

$$SL_n(\mathbb{Z}) \triangleleft GL_n(\mathbb{Z}),$$

siehe auch Beispiel 2.3.7.

Lemma 2.3.10. *Jede Untergruppe* H *von* G *mit* $(G : H) = 2$ *ist normal.*

Beweis. Ist $(G : H) = 2$, dann ist $G = H \cup gH$ als disjunkte Vereinigung. Also ist gH das Komplement von H in G. Das gleiche Argument zeigt, dass auch Hg das Komplement von H in G ist. Also gilt $gH = G \setminus H = Hg$ für alle $g \in G$. □

Beispiel 2.3.11. *Die Untergruppe* $C_n = \{e, r, r^2, \ldots, r^{n-1}\}$ *in* D_n *hat Index 2, and ist deshalb ein Normalteiler.*

Lemma 2.3.12. *Sei* N *ein Normalteiler einer Gruppe* G*. Die Menge der Nebenklassen* G/N *wird mit der Multiplikation* $aN \cdot bN = abN$ *zu einer Gruppe, der sogenannten Faktorgruppe. Die Abbildung* $\pi\colon G \to G/N$, $a \mapsto aN$ *ist ein Gruppenhomomorphismus mit* $\ker(\pi) = N$*.*

Beweis. Die Multiplikation ist wohldefiniert, weil $(ab)N$ nicht von der Wahl der Repräsentanten abhängt. Ist $xN = aN$ und $yN = bN$ für irgenwelche $x, y \in G$, so folgt

$$\begin{aligned}(ab)N &= a(bN) = a(yN) = a(Ny)\\ &= (aN)y = (xN)y = x(Ny)\\ &= x(yN) = (xy)N.\end{aligned}$$

Hier haben wir wesentlich benutzt, dass N normal ist. Man prüft nun die Gruppenaxiome leicht nach. Das neutrale Element von G/N ist $eN = N$, und das Inverse zu aN ist $a^{-1}N$. Wir haben

$$\pi(ab) = abN = aN \cdot bN = \pi(a)\pi(b),$$

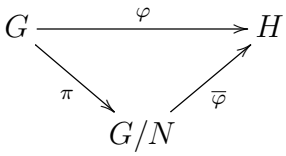
und π ist offensichtlich surjektiv. Es gilt wegen Satz 2.3.1, Teil (c),

$$\begin{aligned}\ker(\pi) &= \{a \in G \mid \pi(a) = eN\}\\ &= \{a \in G \mid aN = eN\}\\ &= \{a \in G \mid a \in N\}\\ &= N.\end{aligned}$$

□

Der Homomorphismus $\pi\colon G \to G/N$ hat eine universelle Eigenschaft.

Satz 2.3.13 (Homomorphiesatz)**.** *Sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus, und N ein Normalteiler von G mit $N \subseteq \ker(\varphi)$. Dann existiert genau ein Gruppenhomomorphismus $\overline{\varphi}\colon G/N \to H$, so dass das Diagramm*



kommutiert, d.h., mit $\varphi = \overline{\varphi} \circ \pi$. Es gilt $\operatorname{im}(\overline{\varphi}) = \operatorname{im}(\varphi)$ und $\ker(\overline{\varphi}) = \pi(\ker(\varphi))$. Insbesondere ist $\overline{\varphi}$ genau dann injektiv, wenn $\ker(\varphi) = N$ gilt.

Beweis. Für jede Abbildung $\overline{\varphi}$ mit $\varphi = \overline{\varphi} \circ \pi$ gilt $\overline{\varphi}(aN) = \varphi(a)$. Daher ist $\overline{\varphi}$ eindeutig bestimmt, falls es existiert. Die Existenz erscheint trivial, weil wir ja $\overline{\varphi}$ einfach durch $\overline{\varphi}(aN) = \varphi(a)$ definieren können. Das macht aber nur dann Sinn, wenn aus $aN = bN$ schon $\varphi(a) = \varphi(b)$ folgt. Das nennt man die *Wohldefiniertheit* von $\overline{\varphi}$, und die müssen wir jetzt zeigen. In der Tat, aus $aN = bN$ folgt $b^{-1}a \in N \subseteq \ker(\varphi)$. Das bedeutet

$$e_H = \varphi(b^{-1}a) = \varphi(b)^{-1}\varphi(a),$$

also $\varphi(a) = \varphi(b)$. Weiterhin gilt

$$\overline{\varphi}(aN)\overline{\varphi}(bN) = \varphi(a)\varphi(b) = \varphi(ab) = \overline{\varphi}(abN) = \overline{\varphi}(aN \cdot bN).$$

Also ist $\overline{\varphi}$ ein Gruppenhomomorphismus. Weiterhin gilt $\operatorname{im}(\overline{\varphi}) = \operatorname{im}(\varphi)$ und $\ker(\overline{\varphi}) = \pi(\ker(\varphi))$ nach Definition. Da π surjektiv ist, ist $\ker(\varphi)$ das Urbild von $\ker(\overline{\varphi})$ unter π, d.h.,

$$\ker(\varphi) = \pi^{-1}(\ker(\overline{\varphi})).$$

Nun ist $\overline{\varphi}$ genau dann injektiv, wenn $\ker(\overline{\varphi}) = N$ trivial ist, d.h., wenn $\ker(\varphi) = \pi^{-1}(N) = N$ ist. □

Korollar 2.3.14. *Sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Dann gilt*

$$G/\ker(\varphi) \cong \varphi(G).$$

Beweis. Nach Satz 2.3.13 mit $N = \ker(\varphi)$ existiert ein eindeutig bestimmter Homomorphismus $\overline{\varphi}\colon G/\ker(\varphi) \to \varphi(G)$ mit $\varphi = \overline{\varphi} \circ \pi$. Er ist injektiv wegen $\ker(\varphi) = N$ und surjektiv wegen $\operatorname{im}(\overline{\varphi}) = \operatorname{im}(\varphi) = \varphi(G)$. Also ist er ein Isomorphismus. □

Beispiel 2.3.15. *Für $G = GL_n(K)$ und $\varphi = \det\colon GL_n(K) \to K^\times$ gilt $\ker(\varphi) = SL_n(K)$ und $\varphi(G) = K^\times$. Also erhalten wir*

$$GL_n(K)/SL_n(K) \cong K^\times.$$

Beispiel 2.3.16. *Sei $G = \langle g \rangle$ eine endliche zyklische Gruppe. Dann ist $\varphi\colon \mathbb{Z} \to G$, $k \mapsto g^k$ ein Gruppenhomomorphismus mit $\ker(\varphi) = m\mathbb{Z}$ für ein $m \in \mathbb{Z}$ und $\varphi(\mathbb{Z}) = G$. Wir erhalten dann*

$$\mathbb{Z}/m\mathbb{Z} \cong G.$$

Für zwei Untergruppen H und N von G bezeichne

$$HN = \{hn \mid h \in H, n \in N\}$$

das Komplexprodukt.

Satz 2.3.17 (1. Isomorphiesatz)**.** *Sei G eine Gruppe, H eine Untergruppe und N ein Normalteiler. Dann ist HN eine Untergruppe von G, N ein Normalteiler in HN und $H \cap N$ ein Normalteiler in H. Die Einbettung $H \subseteq HN$ induziert einen Isomorphismus*

$$H/(H \cap N) \cong HN/N.$$

Beweis. Die Menge HN erfüllt die Untergruppenaxiome (S1) und (S2). Für Elemente $h_1n_1, h_2n_2 \in HN$ gilt

$$(h_1n_1)(h_2n_2) = h_1(n_1h_2)n_2 \in h_1h_2N,$$

weil $n_1h_2 \in Nh_2 = h_2N$ ist, also $n_1h_2 = h_2n$ für ein $n \in N$ gilt. Das zeigt (S1). Für $hn \in HN$ gilt

$$(hn)^{-1} = n^{-1}h^{-1} = (h^{-1}n^{-1}h)h^{-1} \in NH,$$

weil $h^{-1}n^{-1}h = n' \in N$ gilt. Also gilt $(S2)$. Wegen $N \triangleleft G$ gilt erst recht $N \triangleleft HN$. Die Komposition

$$H \hookrightarrow HN \to HN/N$$

ist ein surjektiver Homomorphismus mit Kern $H \cap N$, der deswegen ein Normalteiler in H ist. In der Tat, $\varphi\colon H \to HN/N$ ist durch $h \mapsto hN$ gegeben, mit

$$\begin{aligned}\ker(\varphi) &= \{a \in H \mid aN = N\} \\ &= \{a \in H \mid a \in N\} \\ &= H \cap N.\end{aligned}$$

Aus Korollar 2.3.14 folgt dann

$$H/(H \cap N) \cong HN/N.$$

□

Einen surjektiven Homomorphismus bezeichnet man auch als *Epimorphismus*.

Satz 2.3.18 (2. Isomorphiesatz)**.** *Sei G eine Gruppe, H und N Normalteiler mit $N \subseteq H$. Dann ist N auch Normalteiler in H, und man kann H/N als Normalteiler von G/N auffassen. Es gibt einen Epimorphismus $G/N \to G/H$, der einen Isomorphismus*

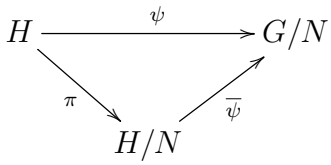
$$(G/N)/(H/N) \cong G/H.$$

induziert.

Beweis. Wegen $N \triangleleft G$ gilt auch $N \triangleleft H$. Die Inklusion $H \hookrightarrow G$ induziert den Homomorphismus

$$\psi\colon H \hookrightarrow G \to G/N,$$

der den Kern N hat. nach dem Homomorphiesatz gibt es also einen eindeutig bestimmen Homomorphismus $\overline{\psi}\colon H/N \to G/N$, so dass das Diagramm



kommutiert, d.h., mit $\psi = \overline{\psi} \circ \pi$. Wegen $\ker(\psi) = N$ ist $\overline{\psi}$ injektiv. Also können wir H/N mit der Untergruppe $\mathrm{im}(\overline{\psi})$ von G/N identifizieren. Der Epimorphismus $G \to G/H$ induziert wegen $N \subseteq H$ auch einen Epimorphismus

$$\varphi\colon G/N \to G/H,\ aN \mapsto aH$$

mit

$$\begin{aligned}\ker(\varphi) &= \{aN \in G/N \mid aH = H\}\\ &= \{aN \in G/N \mid a \in H\}\\ &= H/N.\end{aligned}$$

Nun folgt die Behauptung aus Korollar 2.3.14. □

Beispiel 2.3.19. *Wir haben*

$$(\mathbb{Z}/16\mathbb{Z})/(8\mathbb{Z}/16\mathbb{Z}) \cong \mathbb{Z}/8\mathbb{Z}.$$

2.4 Symmetrische Gruppen

Nach dem Satz von Cayley (Satz 2.2.2) kann jede endliche Gruppe als Untergruppe einer symmetrischen Gruppe aufgefasst werden. Es lohnt sich daher, symmetrische Gruppen und ihre Elemente etwas genauer zu betrachten. Jedes Element $\pi \in S_n$ ist eine Permutation der Zahlen in $X = \{1, 2, \ldots, n\}$, die man zunächst in zweireihiger Notation darstellen kann:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi(1) & \pi(2) & \pi(3) & \cdots & \pi(n) \end{pmatrix}.$$

Es ist aber oft günstiger, π als Produkt von sogenannten *Zykeln* darzustellen.

Definition 2.15. Seien $i_1, \ldots, i_k$ verschiedene ganze Zahlen aus X. Ein Element $\pi \in S_n$ heißt *k-Zykel*, falls

$$\pi(i_1) = i_2, \ldots, \pi(i_{k-1}) = i_k, \pi(i_k) = i_1,$$

und π alle übrigen Elemente aus X fixiert. Man schreibt $\pi = (i_1 \ldots i_k)$. Wir nennen $\{i_1, \ldots, i_k\}$ den *Träger* des k-Zykels.

Ein 1-Zykel fixiert alle $i \in X$, also haben wir $(i) = \mathrm{id}$. Ein 2-Zykel (ij) heißt auch *Transposition*. Wegen $(ij)^2 = \mathrm{id}$ hat eine Transposition die Ordnung 2 in der Gruppe S_n. Allgemeiner hat ein k-Zykel die Ordnung k.

Bemerkung 2.4.1. Je zwei Zykel $\sigma, \tau \in S_n$ mit disjunkten Trägern kommutieren, d.h., $\sigma\tau = \tau\sigma$.

Lemma 2.4.2. *Sei $\alpha = (i_1 \cdots i_k)$ ein k-Zykel und $\tau \in S_n$. Dann ist $\tau\alpha\tau^{-1}$ wieder ein k-Zykel, gegeben durch*

$$\tau\alpha\tau^{-1} = (\tau(i_1) \cdots \tau(i_k)).$$

Beweis. Wegen $(\tau^{-1}\tau)(i_r) = i_r$ und $\alpha(i_r) = i_{r+1 \bmod k}$ gilt

$$\tau\alpha\tau^{-1}(\tau(i_r)) = \tau(i_{r+1 \bmod k})$$

für alle $1 \leq r \leq k$. Sei $1 \leq j \leq n$ gegeben mit $j \neq i_r$ für jedes r. Dann ist $\alpha(j) = j$, weil j nicht im k-Zykel α enthalten ist. Also ist $\tau\alpha\tau^{-1}(\tau(j)) = \tau(j)$, und $\tau\alpha\tau^{-1}$ fixiert jede Zahl, die nicht von der Form $\tau(i_r)$ ist für ein i, und wir haben

$$\tau\alpha\tau^{-1} = (\tau(i_1) \cdots \tau(i_k)).$$

□

Nicht jede Permutation ist ein Zykel, aber jede Permutation kann, im wesentlichen eindeutig, als Produkt von Zyklen geschrieben werden:

Satz 2.4.3 (Zykelzerlegung)**.** *Sei $\sigma \in S_n$. Dann gibt es ein $r \in \mathbb{N}$ und Zyklen $\sigma_1, \ldots, \sigma_r$ der Länge mindestens zwei mit paarweise disjunkten Trägern und*

$$\sigma = \sigma_1 \cdots \sigma_r.$$

Dabei sind r und $\{\sigma_1, \ldots, \sigma_r\}$ eindeutig durch σ bestimmt.

Der Satz folgt leicht durch Induktion über die Anzahl der $i \in X$, die durch σ nicht fixiert werden, und ist dem Leser als Übung überlassen.

Beispiel 2.4.4.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 4 & 2 & 1 & 3 & 6 & 8 \end{pmatrix} = (15)(27634)(8).$$

Satz 2.4.5. *Jedes $\sigma \in S_n$ ist für $n \geq 2$ ein Produkt von Transpositionen.*

Beweis. Wegen Satz 2.4.3 genügt es zu zeigen, dass jeder k-Zykel ein Produkt von Transpositionen ist. Für $k = 1$ gilt $(1) = (12)^2$, und für $k \geq 2$ gilt

$$(i_1 i_2 \cdots i_k) = (i_1 i_2)(i_2 i_3) \cdots (i_{k-1} i_k).$$

□

Beispiel 2.4.6.

$$(13526) = (13)(35)(52)(26).$$

Definition 2.16. Das *Signum* von $\pi \in S_n$ ist definiert durch

$$sgn(\pi) = \prod_{i<j} \frac{\pi(i) - \pi(j)}{i - j}.$$

Es definiert eine Abbildung $sgn\colon S_n \to \{\pm 1\}$ durch $\pi \mapsto sgn(\pi)$.

Satz 2.4.7. *Die Abbildung* $sgn\colon S_n \to C_2$ *ist ein Gruppenhomomorphismus, d.h.,*

$$sgn(\sigma\tau) = sgn(\sigma)sgn(\tau)$$

für alle $\sigma, \tau \in S_n$.

Den Beweis kennen wir aus der linearen Algebra.

Definition 2.17. Die *alternierende Gruppe* A_n ist definiert als der Kern des Signum-Homomorphismus.

Offenbar gilt $A_1 = A_2 = 1$ und $|A_n| = \frac{n!}{2}$ für $n \geq 2$. Als Kern ist A_n ein Normalteiler von S_n mit Faktorgruppe $S_n/A_n \cong C_2$. Da Transpositionen das Signum -1 haben, liegen sie nicht in A_n. Aber alle Elemente, die ein Produkt von einer geraden Anzahl von Transpositionen sind, liegen in A_n. Umgekehrt sind alle Elemente von A_n ein (eventuell leeres) Produkt von einer geraden Anzahl von Transpositionen, siehe Satz 2.4.5.

Lemma 2.4.8. *Jedes Element von* A_n, $n \geq 3$ *ist ein Produkt von* 3*-Zykeln. Also wird* A_n *von* 3*-Zykeln erzeugt.*

Beweis. Es gilt $(1) = (123)^3$. Jedes $\pi \in A_n$ ist ein Produkt von einer geraden Anzahl von Transpositionen. Aber das Produkt von je zwei Transpositionen kann immer als Produkt von 3-Zykeln geschrieben werden. Entweder ist $(ij)(ij) = (1)$, oder $(ij)(jl) = (ijl)$, oder

$$(ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl)$$

für paarweise verschiedene i, j, k, l. □

Beispiel 2.4.9. *Wir haben* $A_3 = \{(1), (123), (132)\}$. *Wegen Korollar* 2.3.5 *ist jede Gruppe der Ordnung* 3 *isomorph zu* C_3*, d.h.,* $A_3 \cong C_3$.

2.5 Gruppen kleiner Ordung

Wir möchten mit elementaren Mitteln alle Gruppen der Ordung $n \leq 8$ bis auf Isomorphie bestimmen. Zunächst einmal gibt es zu jedem $n \in \mathbb{N}$ eine zyklische Gruppe der Ordnung n, nämlich C_n. Zudem kennen wir schon die S_3 mit 6 Elementen, und die D_4 mit 8 Elementen. Wir können auch direkte Produkte von diesen Gruppen betrachten. Wir benötigen noch eine andere wichtige Gruppe der Ordnung 8.

Definition 2.18. Sei Q_8 die von

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

erzeugte Untergruppe von $GL_2(\mathbb{C})$. Sie heißt *Quaternionengruppe*.

Es gilt

$$K = IJ = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = -JI$$

und $J^2 = I^2 = K^2 = -E$, also $J^4 = I^4 = K^4 = E$. Somit besteht Q_8 aus den Matrizen

$$\begin{aligned} Q_8 &= \{E, -E, I, -I, J, -J, K, -K\} \\ &= \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right), \left(\begin{smallmatrix} -i & 0 \\ 0 & i \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & -i \\ -i & 0 \end{smallmatrix}\right)\}. \end{aligned}$$

Da Gruppen der Ordnung p mit p prim isomorph zu C_p sind, gibt es je eine Gruppe der Ordnung $1, 2, 3$. Für $|G| = 4$ gibt es mehr als nur eine Gruppe.

Satz 2.5.1. *Jede Gruppe der Ordnung* 4 *ist isomorph zu* C_4 *oder* $C_2 \times C_2$.

Beweis. Sei G eine Gruppe der Ordnung 4. Falls G ein Element der Ordnung 4 hat, gilt $G \cong C_4$. Andernfalls gilt $G = \{e, a, b, c\}$ und die Ordnung von a, b, c ist ein echter Teiler von 4 nach Lagrange, aber nicht 1, weil die Elemente verschieden von e sind. Also haben a, b, c die Ordnung 2 und es gilt $a^2 = b^2 = c^2 = e$. Wir behaupten, dass $ab = c$ gilt, weil alle anderen Wahlen für ab unmöglich sind. Aus $ab = e$ würde zum Beispiel $a = b^{-1}$ folgen, also $b = b^{-1} = a$, ein Widerspruch. $ab = a$ würde $b = e$ bedeuten und $ab = b$ wiederum $a = e$. In der gleichen Weise sehen wir, dass $ba = c = ab, ca = b = ac$ und $cb = a = bc$ gilt. Mit diesen Relationen und $C_2 = \{\pm 1\}$ sieht man leicht, dass die Abbildung $f\colon G \to C_2 \times C_2$ mit

$$f(e) = (1, 1),\ f(a) = (-1, 1),\ f(b) = (1, -1),\ f(c) = (-1, -1)$$

ein Isomorphismus ist. □

Satz 2.5.2. *Jede Gruppe gerader Ordnung hat eine ungerade Anzahl von Elementen der Ordnung* 2.

Beweis. Für $a \in G$ sei $U_a = \{a, a^{-1}\}$. Es gilt $|U_a| = 2$, außer für Elemente der Ordnung 1 und 2, wo $a = a^{-1}$ gilt. Sei k die Anzahl der Elemente der Ordnung 2 in G. Es gibt genau ein Element der Ordnung 1. Wir haben die disjunkte Vereinigung

$$G = \bigcup_{a \in G} U_a$$

und somit

$$|G| = \sum_{a \in G} |U_a| = |U_e| + k \cdot 1 + \ell \cdot 2.$$

Wegen $|U_e| = 1$ muss k ungerade sein. □

Wir wollen diesen Satz auf Gruppen der Ordnung 6 anwenden.

Lemma 2.5.3. *Sei G eine Gruppe der Ordnung 6. Dann besitzt G ein Element der Ordnung 2 und ein Element der Ordnung 3.*

Beweis. Hat G ein Element der Ordnung 6, so ist $G \cong C_6 \cong C_2 \times C_3$, und die Behauptung ist richtig. Andernfalls haben alle Elemente außer e die Ordnung 2 oder 3 wegen Lagrange. Nach Satz 2.5.2 gibt es 1, 3 oder 5 Elemente der Ordnung 2. Angenommen, es gäbe 5 solche Elemente. Dann hätte G mindestens drei Erzeuger a, b, c, denn für 2 Erzeuger der Ordnung 2 wäre $G \cong C_2 \times C_2$. Dann wären aber auch alle Elemente a, b, c, ab, ac, bc, abc verschieden wegen der Kürzungsregel. Somit wäre

$$G = \{e, a, b, c, ab, ac, bc, abc\} \cong C_2 \times C_2 \times C_2,$$

und G hätte mehr als 6 Elemente, ein Widerspruch. Also hat G ein oder drei Elemente der Ordung 2 und mindestens ein Element der Ordnung 3. □

Satz 2.5.4. *Jede Gruppe der Ordnung 6 ist isomorph zu C_6 oder S_3.*

Beweis. Wegen Lemma 2.5.3 gibt es Elemente $a, b \in G$ mit $\mathrm{ord}(a) = 2$ und $\mathrm{ord}(b) = 3$. Dann sind die Elemente e, a, b, ab, b^2, ab^2 wegen den Kürzungsregeln alle verschieden. Da G sechs Elemente hat, folgt

$$G = \{e, a, b, ab, b^2, ab^2\}.$$

Nun bestimmen wir ba. Es muss eines der 6 Elemente sein. $ba = e$ ist unmöglich, da sonst $b = a^{-1}$ und $2 = \mathrm{ord}(a) = \mathrm{ord}(a^{-1}) = \mathrm{ord}(b) = 3$. $ba = a$ oder $ba = b$ würde $b = e$ oder $a = e$ bedeuten. Auch $ba = b^2$ ist unmöglich. Angenommen, $ba = ab$. Dann besteht die Gruppe genau aus den Elementen $\{a^i b^j \mid i = 0, 1,\ j = 0, 1, 2\} = C_2 \times C_3 \cong C_6$. Andernfalls gilt $ba = ab^2 = ab^{-1}$. Das ist genau die Definition von D_3. Mit $a = (12)$ und $b = (123)$ ist das die Gruppe S_3, wie wir schon gesehen haben. □

Lemma 2.5.5. *Jede abelsche Gruppe der Ordnung 8 ist isomorph zu C_8, $C_2 \times C_4$ oder $C_2 \times C_2 \times C_2$.*

Beweis. Ohne die Klassifikation endlich-erzeugter abelscher Gruppen zu verwenden, kann man wie folgt argumentieren. Falls G ein Element der Ordung 8 hat, gilt $G \cong C_8$. Wenn G kein Element der Ordnung 4 hat, so haben alle Elemente außer e die Ordnung 2 und wir erhalten $G \cong C_2 \times C_2 \times C_2$ wie in Beweis von Lemma 2.5.3. Es bleibt der Fall, das G ein Element a mit $\mathrm{ord}(a) = 4$ hat. Sei $N = \langle a \rangle$ und b irgendein Element in $G \setminus N$. Dann ist $bN \neq N$ und

$$G = N \cup bN = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Angenommen, alle Elemente in $G \setminus N$ hätten Ordnung 4. Dann hätte b^2 die Ordnung 2, weswegen dann $b^2 \in N$ gälte. Aber das einzige Element der Ordnung 2 in N ist a^2, also hat man $a^2 = b^2$ und mit $a^4 = e$ dann

$$(a^3b)^2 = a^3ba^3b = a^6b^2 = a^8 = e.$$

Das ist ein Widerspruch zu $\mathrm{ord}(a^3b) = 4$. Also gibt es doch ein Element b der Ordnung 2 in $G \setminus N$. Wir haben $N = \langle a \rangle \cong C_4$ und $K = \langle b \rangle \cong C_2$, und G ist das direkte Produkt beider Gruppen. In der Tat gilt $N \cap K = 1$, $N, K \trianglelefteq G$ und $NK = G$, wegen

$$|NK| = \frac{|N||K|}{|N \cap K|} = \frac{4 \cdot 2}{1} = 8.$$

Also ist $G \cong N \times K \cong C_4 \times C_2$. □

Satz 2.5.6. *Jede nicht-abelsche Gruppe der Ordnung 8 ist isomorph zu D_4 oder Q_8.*

Beweis. Da G nicht-abelsch ist, haben alle Elemente bis auf e die Ordnung 2 oder 4. Gilt $g^2 = e$ für alle $g \in G$ dann ist G abelsch. Also gibt es ein Element $x \in G$ der Ordnung 4. Sei $y \in G \setminus \langle x \rangle$. Die Untergruppe $\langle x, y \rangle$ enthält $\langle x \rangle$ als echte Teilmenge, also gilt $\langle x, y \rangle = G$. Nach Vorraussetzung kommutieren x und y nicht. Da $\langle x \rangle$ Index 2 in G hat, ist es ein Normalteiler. Also gilt

$$yxy^{-1} \in \langle x \rangle = \{e, x, x^2, x^3\}.$$

Da yxy^{-1} Ordnung 4 hat, folgt $yxy^{-1} = x$ oder $yxy^{-1} = x^3 = x^{-1}$. Der erste Fall isr unmöglich, denn x und y kommutieren nicht. Also gilt $yxy^{-1} = x^{-1}$. Die Gruppe $G/\langle x \rangle$ hat Ordnung 2, also gilt

$$y^2 \in \langle x \rangle = \{e, x, x^2, x^3\}.$$

Da y Ordnung 2 oder 4 hat, hat y^2 Ordnung 1 oder 2. Also $y^2 = 1$ oder $y^2 = x^2$. Also haben wir $G = \langle x, y \rangle$ mit entweder

$$x^4 = e, y^2 = e, yxy^{-1} = x^{-1},$$

oder

$$x^4 = e, y^2 = x^2, yxy^{-1} = x^{-1}.$$

Es ist nun leicht zu sehen, dass $G \cong D_4$ im ersten Fall, und $G \cong Q_8$ im zweiten Fall. □

Sei $f(n)$ die Anzahl der nicht-isomorphen Gruppen der Ordnung n. Dann ist die Klassifikation der Gruppen mit $n \leq 8$ wie folgt gegeben:

n	$f(n)$	Gruppen
1	1	1
2	1	C_2
3	1	C_3
4	2	$C_4, C_2 \times C_2$
5	1	C_5
6	2	C_6, S_3
7	1	C_7
8	5	$C_8, C_2 \times C_4, C_2 \times C_2 \times C_2, Q_8, D_4$

Bemerkung 2.5.7. Die Resultate in diesem Abschnitt sind Spezialfälle allgemeinerer Resultate. Satz 2.5.1 kann für alle Gruppen der Ordnung p^2 verallgemeinert werden. Es gibt genau zwei verschiedene Gruppen der Ordnung p^2, nämlich $C_p \times C_p$ und C_{p^2}. Lemma 2.5.3 ist ein Spezialfall des Satzes von *Cauchy*: für jede Primzahl p, die die Gruppenordnung teilt, gibt es ein Element der Ordnung p in G. Auch Satz 2.5.4 gilt allgemeiner: jede Gruppe der Ordnung $2p$ für eine ungerade Primzahl p ist isomorph zu C_{2p} oder D_p.

Bemerkung 2.5.8. Die Funktion $f(n)$ hat in der *Online Encyclopedia of Integer Sequences* OEIS sogar die erste Nummer, nämlich A000001. Diese Funktion wächst rasant für Primzahlpotenzen p^n, siehe Higman's Arbeit [3]. In der Tat haben wir

$$p^{\frac{2}{27}n^2(n-6)} \leq f(p^n) \leq p^{\frac{2}{27}n^3+O(n^{5/2})}$$

Was die Klassifikation von endlichen Gruppen im allgemeinen betrifft, so gibt es das *Millennium-Projekt* von Besche, Eick und O'Brian [1]. Sie haben alle Gruppen der Ordnung $n \leq 2000$ klassifiziert. Die Arbeit wurde 2002 publiziert. Die meisten Gruppen gibt es tendenziell für Potenzen von 2. Es gibt genau 49.910.529.484 verschiedene Gruppen der Ordnung $n \leq 2000$. Mehr als 99% von ihnen haben die Ordnung 2^{10}. Es gilt $f(2^{10}) = 49.487.365.422$. Die anderen Werte für $f(2^k)$, mit $k = 1, \ldots 9$ sind

$$1,\ 2,\ 5,\ 14,\ 51,\ 267,\ 2328,\ 56092,\ 10494213.$$

2.6 Gruppenoperationen

Definition 2.19. Sei G eine Gruppe und X eine Menge. Eine *Gruppenoperation* von G auf X ist eine Abbildung $(g, x) \mapsto gx$, $G \times X \to X$ mit

(1) $g(hx) = (gh)x$ für alle $g, h \in G$ und alle $x \in X$,

(2) $ex = x$ für das neutrale Element $e \in G$ und alle $x \in X$.

Eine Gruppenoperation von G auf X ist nichts anderes als ein Gruppenhomomorphismus $G \to \mathrm{Sym}(X)$. Die Operation definiert nämlich Linksmultiplikationen $L_g \in \mathrm{Sym}(X)$, und die Axiome besagen dann, daß $L\colon G \to \mathrm{Sym}(X)$, $g \mapsto L(g) = L_g$ ein Homomorphismus ist.

Die Operation hießt *treu*, falls L injektiv ist, d.h., falls gilt

$$gx = x \text{ für alle } x \in X \text{ impliziert } g = e.$$

Beispiel 2.6.1. 1. *Jede Gruppe G operiert auf jeder Menge X durch die triviale Operation, d.h., durch $gx = x$ für alle $g \in G$ und alle $x \in X$.*

2. *Die Gruppe $GL_n(K)$ operiert auf K^n durch Matrix Multiplikation, also durch $(A, x) \mapsto Ax$.*

3. *Die symmetrische Gruppe S_n operiert durch Permutationen auf der Menge $X = \{1, 2, \ldots, n\}$.*

4. *Jede Gruppe G operiert auf sich selbst durch Konjugation: mit $X = G$ ist die Operation durch $(g, x) \mapsto gxg^{-1}$ gegeben.*

5. *Für jede Gruppe G operiert die Automorphismengruppe $\mathrm{Aut}(G)$ auf G.*

6. *Die Gruppe $SL_2(\mathbb{C})$ der komplexen 2×2-Matrizen $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ mit Determinante $\det(A) = 1$ operiert auf der Riemannschen Zahlenkugel $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ durch Möbius Transformationen*

$$(A, z) \mapsto A \cdot z = \frac{az + b}{cz + d},$$

mit $A \cdot \infty = a/c$ und $A \cdot (-d/c) = \infty$.

Wir wollen die Axiome für das letzte Beispiel nachprüfen. Die Einheitsmatrix I operiert durch $Iz = \frac{1z+0}{0z+1} = z$. Für zwei Matrizen $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ hat man

$$\begin{aligned} A \cdot (B \cdot z) = A \cdot \left(\frac{\alpha z + \beta}{\gamma z + \delta}\right) &= \frac{a\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) + b}{c\left(\frac{\alpha z+\beta}{\gamma z+\delta}\right) + d} \\ &= \frac{(a\alpha + b\gamma)z + (a\beta + b\delta)}{(c\alpha + d\gamma)z + (c\beta + d\delta)} \\ &= \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix} \cdot z \\ &= (AB) \cdot z. \end{aligned}$$

Definition 2.20. Sei G eine Gruppe, die auf einer Menge X operiert. Für $x \in X$ heißt die Menge

$$Gx = \{gx \mid g \in G\} \subseteq X$$

die *Bahn* von x. Man sagt auch G-Orbit und schreibt $O(x)$.

Beispiel 2.6.2. *Operiert G auf such selbst durch Konjugation, so sind die G-Orbiten nichts anderes als die Konjugationsklassen. Hier ist für $x \in X = G$ die Konjugationsklasse von x die Menge*

$$\{gxg^{-1} \mid g \in G\}.$$

Zwei Bahnen Gx und Gy sind entweder disjunkt oder gleich, denn aus

$$gx = hy \in Gx \cap Gy$$

folgt $x = g^{-1}hy$, also $Gx \subseteq Gy$, und $y = h^{-1}gx$, also $Gy \subseteq Gx$. Also ist X die disjunkte Vereinigung aller Bahnen.

Definition 2.21. Sei G eine Gruppe, die auf einer Menge X operiert. Für $x \in X$ heißt die Menge

$$G_x = \{g \in G \mid gx = x\} \subseteq G$$

der *Stabilisator* von x, oder die Isotropiegruppe von x.

In der Tat ist G_x eine Untergruppe von G, aber im allgemeinen kein Normalteiler.

Beispiel 2.6.3. *Operiert G auf such selbst durch Konjugation, so sind die Stabilisatoren gerade die* Zentralisatoren. *Hier ist für $x \in X$ der* Zentralisator *von x in G die Menge*

$$C_G(x) = \{g \in G \mid gx = xg\}.$$

Das Zentrum $Z(G)$ von G ist gerade der Schnitt über alle Zentralisatoren,

$$Z(G) = \bigcap_{x \in G} C_G(x) = \{g \in G \mid gx = xg \; \forall \, x \in G\}.$$

Beispiel 2.6.4. *Sei G eine Gruppe, die durch Konjugation auf sich selbst operiert und H eine Untergruppe von G. Dann ist der Stabilisator von H genau der Normalisator von H in G. Hier ist der* Normalisator $N_G(H)$ *von H in G gegeben durch*

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Definition 2.22. Eine Gruppenoperation einer Gruppe G auf einer nicht-leeren Menge X heißt *transitiv*, falls es nur eine Bahn gibt, d.h., falls für alle $x, y \in X$ ein $g \in G$ existiert mit $gx = y$.

Dann ist $Gx = X$ für alle $x \in X$.

Beispiel 2.6.5. *1. Die Gruppe S_n operiert transitiv auf $X = \{1, 2, \ldots, n\}$.*

2. Die Konjugationsoperation einer nicht-trivialen Gruppe G ist nicht transitiv.

3. Die Operation von $GL_n(K)$ auf K^n durch Matrix Multiplkation ist nicht transitiv.

Für 1. benutze man, dass 1 auf jede Zahl in X abbildet werden kann unter einer Permutation von S_n. Wäre die Operation in 2. transitiv, so wäre jeder Orbit gleich G. Wegen $g \cdot e = geg^{-1} = e$ wäre also G trivial, Widerspruch. Für 3. genügt es zu bemerken, dass die Bahn von 0 nicht gleich X ist.

2.7 Die Klassengleichung

Definition 2.23. Sei G eine Gruppe, die auf X operiert. Eine G-invariante Abbildung zwischen G-Mengen X und Y ist eine Abbildung $\varphi\colon X \to Y$ mit $\varphi(gx) = g\varphi(x)$ für alle $x \in X$ und alle $g \in G$. Die Abbildung φ heißt *Isomorphismus von G-Mengen*, falls φ bijektiv und G-invariant ist.

Theorem 2.7.1 (Orbit-Stabilisator-Theorem)**.** *Sei G eine Gruppe, die auf X operiert. Dann ist die Abbildung*

$$\varphi\colon G/G_x \to Gx,\ gG_x \mapsto gx$$

ein Isomorphismus von G-Mengen und es gilt

$$|Gx| = (G : G_x) = \frac{|G|}{|G_x|}.$$

Beweis. Die Abbildung φ ist wohldefiniert: aus $gG_x = hG_x$ folgt $g^{-1}h \in G_x$, also $gx = g(g^{-1}hx) = hx$. Sie ist injektiv, weil aus $gx = hx$ folgt $g^{-1}hx = x$, also $g^{-1}h \in G_x$ und deshalb $gG_x = hG_x$. Sie ist surjektiv nach Konstruktion. Wir überlassen es dem Leser zu zeigen, dass die Abbildung G-invariant ist. □

Für die Konjugationsoperation von G auf sich selbst und einer Untergruppe H von G erhält man das folgende Resultat.

Korollar 2.7.2. *Die Anzahl der Konjugierten gHg^{-1} einer Untergruppe H von G ist durch $(G : N_G(H))$ gegeben.*

Da X die disjunkte Vereinigung seiner G-Bahnen ist, folgt aus $|Gx| = (G : G_x)$ die *Bahnengleichung*:

Korollar 2.7.3 (Bahnengleichung)**.** *Ist $(x_i)_{i\in I}$ ein Vertretersystem für die G-Bahnen in X, so gilt*

$$|X| = \sum_{i\in I} (G : G_{x_i}).$$

Die Bahnengleichung wird zur *Klassengleichung* für die Konjugationsoperation.

Satz 2.7.4 (Klassengleichung)**.**

$$\begin{aligned} |G| &= \sum_{x\in\mathcal{C}} (G : C_G(x)) \\ &= |Z(G)| + \sum_{y\in\mathcal{C}'} (G : C_G(y)), \end{aligned}$$

wobei x ein Vertretersystem $\mathcal{C}$ für die Konjugationsklassen durchläuft, und y ein Vertretersystem $\mathcal{C}'$ für die Konjugationsklassen mit mehr als einem Element.

Man beachte, dass jeder Summand ein Teiler von $|G|$ ist, also jede Konjugationsklasse eine Ordung hat, die ein Teiler von $|G|$ ist. Das folgt nicht aus Lagrange, da Konjugationsklassen keine Untergruppen sein müssen.

Die folgende Tabelle zeigt die Konjugationsklassen in S_4. Sie sind durch den Zykeltyp bestimmt.

Zykeltyp	Elemente
1	(1)
(ab)	$(12), (13), (14), (23), (24), (34)$
(abc)	$(123), (132), (124), (142), (134), (143), (234), (243)$
$(ab)(cd)$	$(12)(34), (13)(24), (14)(23)$
$(abcd)$	$(1234), (1432), (1324), (1423), (1243), (1342)$

Beispiel 2.7.5. *Die Klassengleichung für S_4 lautet*

$$|S_4| = 24 = 1 + 6 + 8 + 3 + 6.$$

Wir haben $Z(S_4) = 1$.

Die Klassengleichung hat einige wichtige Konsequenzen. Zunächst wollen wir die Klassifikation endlicher abelscher Gruppen aus der elementaren Zahlentheorie in Erinnerung rufen.

Theorem 2.7.6. *Sei A eine endliche abelsche Gruppe. Dann gibt es ein $k \in \mathbb{N}$, Primzahlen $p_1, \ldots, p_k$ und positive ganze Zahlen $n_1, \ldots, n_k$ mit*

$$A \cong \prod_{j=1}^{k} \mathbb{Z}/p_j^{n_j}\mathbb{Z}.$$

Dabei sind k und die Paare (p_j, n_j) bis auf Reihenfolge eindeutig durch A bestimmt.

Korollar 2.7.7. *Sei A eine endliche abelsche Gruppe und p eine Primzahl, die $|A|$ teilt. Dann besitzt A ein Element der Ordnung p.*

Beweis. Wegen $|A| = \prod_{j=1}^{k} p_j^{n_j}$ bedeutet $p \mid |A|$, dass $p = p_i$ für ein i. Also hat A eine Untergruppe, die isomorph zu einer zyklischen Gruppe $\mathbb{Z}/p^n\mathbb{Z}$ ist. Ihr Erzeuger g hat Ordnung p^n. Dann hat das Element $g^{p^{n-1}}$ die Ordung p, denn $\operatorname{ord}(g^k) = \frac{n}{\gcd(k,n)}$ in einer zyklischen Gruppe der Ordung n. □

Nun folgt mit Hilfe der Klassengleichung eine Verallgemeinerung, die als der Satz von Cauchy bekannt ist.

Satz 2.7.8 (Cauchy)**.** *Sei G eine endliche Gruppe und p eine Primzahl, die $|G|$ teilt. Dann besitzt G ein Element der Ordnung p.*

Beweis. Wir machen eine Induktion über $|G|$. Angenommen, es gibt ein Element $y \in G \setminus Z(G)$ mit $p \nmid (G : C_G(y))$. Dann folgt $p \mid |C_G(y)|$ wegen

$$(G : 1) = (G : C_G(y)) \cdot (C_G(y) : 1).$$

Nach Induktionsannahme gibt es ein Element der Ordung p in $C_G(y)$, und somit auch in G. Also dürfen wir annehmen, dass p *alle* Terme $(G : C_G(y))$ in der Klassengleichung für nicht-zentrale Elemente y teilt. Aber dann haben wir $p \mid |Z(G)|$. Da $Z(G)$ abelsch ist, gibt es wegen Korollar 2.7.7 ein Element der Ordnung p in $Z(G) \subseteq G$. □

Der Satz von Cauchy ist sehr nützlich für die Strukturtheorie endlicher Gruppen.

Satz 2.7.9. *Jede Gruppe der Ordnung $2p$ für eine Primzahl $p > 2$ ist isomorph zu C_{2p} oder D_p.*

Beweis. Nach Cauchy's Theorem gibt es für jeden Primteiler p von $|G|$ ein Element der Ordung p in G. Wegen $|G| = 2p$ und $p > 2$ können wir das für 2 und p anwenden. Sei s also ein Element der Ordnung 2, und r ein Element der Ordnung p. Dann ist $C_p = \langle r \rangle$ ein Normalteiler von G wegen $(G : C_p) = 2$, siehe Lemma 2.3.10. Offensichtlich gilt $s \notin C_p$, so dass $G = C_p \cup C_p s$. Das bedeutet $G = \{1, r, \ldots, r^{p-1}, s, rs, \ldots, r^{p-1}s\}$. Da C_p normal ist gilt $srs^{-1} = r^k$ für ein $k \in \mathbb{Z}$. Wegen $s^2 = e$ haben wir

$$r = s^2 r s^{-2} = s(srs^{-1})s^{-1} = r^{k^2}.$$

Das bedeutet $k^2 \equiv 1 \mod p$, also $p \mid (k-1)(k+1)$. Es folgt also entweder $k \equiv 1 \mod p$ oder $k \equiv -1 \mod p$. In ersten Fall ist G abelsch (jede Gruppe, die durch kommutierende Elemente erzeugt wird, ist kommutativ), d.h., $G = \langle r, s \mid r^p = s^2 = e, rs = sr \rangle \cong C_{2p}$. Im zweiten Fall haben wir $srs^{-1} = r^{-1}$, so dass $G \cong D_p$. □

Definition 2.24. Eine endliche Gruppe G heißt *p-Gruppe*, falls sie Primzahlpotenzordnung hat, d.h., falls $|G| = p^m$.

Satz 2.7.10. *Eine endliche Gruppe G ist genau dann eine p-Gruppe falls jedes Element eine p-Potenz Ordung hat.*

Beweis. Ist $|G| = p^m$, dann hat wegen des Satzes von Lagrange jedes Element eine Ordnung, die p^m teilt, also eine p-Potenz ist. Für die Umkehrung nehmen wir an, es gäbe eine Primzahl $q \neq p$ mit $q \mid |G|$. Dann gäbe es ein Element $g \in G$ mit $\mathrm{ord}(g) = q \neq p^k$ wegen Cauchys Theorem. Das ist ein Widerspruch zur Voraussetzung. Also gilt $|G| = p^m$ für ein $m \in \mathbb{N}$. □

Satz 2.7.11. *Sei G eine nicht-triviale endliche p-Gruppe. Dann ist $Z(G)$ nicht-trivial.*

Beweis. Nach Voraussetzung ist $(G : 1)$ eine p-Potenz. Also sind alle Terme über $y \in \mathcal{C}'$ in der Klassengleichung durch p teilbar. Das bedeutet $p \mid |Z(G)|$. □

Satz 2.7.12. *Eine Gruppe der Ordnung p^n hat Normalteiler von jeder möglichen Ordnung $1, p, \ldots, p^n$.*

Beweis. Wir machen eine Induktion über n. Wegen Korollar 2.7.7 besitzt $Z(G)$ ein Element g der Ordnung p. Also ist $N = \langle g \rangle$ ein Normalteiler der Ordnung p. Es gilt $|G/N| = p^{n-1}$, und wir können die Induktionsvoraussetzung anwenden. Da die Normalteiler von G/N zu den Normalteilern von G, die N enthalten korrespondieren, folgt die Behauptung für G. □

Lemma 2.7.13. *Sei H eine Untergruppe von G mit $H \subseteq Z(G)$, so dass G/H zyklisch ist. Dann ist G abelsch.*

Beweis. Sei a ein Element in G, dessen Bild in G/H ein Erzeuger ist. Dann kann man jedes Element von G schreiben als $g = a^j h$ mit $h \in H$ und $j \in \mathbb{Z}$. Wegen $H \subseteq Z(G)$ haben wir

$$\begin{aligned} a^i h \cdot a^j h' &= a^i a^j h h' \\ &= a^j a^i h' h \\ &= a^j h' \cdot a^i h. \end{aligned}$$

□

Satz 2.7.14. *Jede Gruppe der Ordnung p^2 mit einer Primzahl p ist abelsch und deshalb isomorph zu $C_p \times C_p$ oder C_{p^2}.*

Beweis. Wegen Lagrange gilt $|Z(G)| \in \{1, p, p^2\}$ und wegen Satz 2.7.11 können wir Ordnung 1 ausschliessen, d.h., $|G/Z(G)| \in \{1, p\}$. In beiden Fällen ist $G/Z(G)$ zyklisch, so dass G abelsch ist wegen Lemma 2.7.13. □

Gruppen der Ordnung p^3 müssen nicht notwenig abelsch sein, wie wir in Satz 2.5.6 für $p = 2$ gesehen haben. Zusammen mit Lemma 2.5.5, oder mit Theorem 2.7.6 haben wir folgende Klassifikation.

Satz 2.7.15. *Jede Gruppe G der Ordnung 2^3 ist isomorph zu einer der Gruppen $C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$ oder D_4, Q_8.*

Auch für $p > 2$ gibt es nicht-abelsche Gruppen der Ordnung p^3. Die *Heisenberggruppe* über $\mathbb{Z}/(p)$ ist definiert durch

$$\mathrm{Heis}(\mathbb{Z}/(p)) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}/(p) \right\}.$$

Sie ist offensichtlich nicht-abelsch und hat die Ordnung p^3. Für $p = 2$ erhält man $\mathrm{Heis}(\mathbb{Z}/(2)) \cong D_4$. Für $p > 2$ haben alle nicht-trivialen Elemente in $\mathrm{Heis}(\mathbb{Z}/(p))$ die Ordnung p, da

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & 0 & \frac{p(p-1)}{2} ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I,$$

weil $\frac{p(p-1)}{2} \equiv 0 \bmod p$ für alle $p > 2$. Eine weitere nicht-abelsche Gruppe der Ordnung p^3 ist wie folgt gegeben. Sei

$$\mathrm{Aff}(\mathbb{Z}/(p^2)) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{Z}/(p^2), a \neq 0 \right\} \subseteq GL_2(\mathbb{Z}/(p^2))$$

die *affine Gruppe* über $\mathbb{Z}/(p^2)$. Sie hat die Ordnung $p^2\varphi(p^2) = p^3(p-1)$ und besitzt einen eindeutigen Normalteiler $\Gamma(p)$ der Ordnung p^3, gegeben durch

$$\Gamma(p) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{Z}/(p^2), a^p = 1 \text{ in } (\mathbb{Z}/(p^2))^\times \right\}.$$

Er ist der Kern des Homomorphismus $\mathrm{Aff}(\mathbb{Z}/(p^2)) \to (\mathbb{Z}/(p^2))^\times$ gegeben durch

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mapsto a^p,$$

und hat ein Element der Ordnung p^2, nämlich $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Deshalb sind $\Gamma(p)$ und $\mathrm{Heis}(\mathbb{Z}/(2))$ für $p > 2$ nicht isomorph. Für $p = 2$ sind sie allerdings beide isomorph zu D_4.

Theorem 2.7.16 (Hölder 1893)**.** *Jede Gruppe der Ordnung p^3 für eine Primzahl $p > 2$ ist isomorph zu einer der Gruppen $C_p \times C_p \times C_p$, $C_p \times C_{p^2}$, C_{p^3},* $\mathrm{Heis}(\mathbb{Z}/p)$ *oder $\Gamma(p)$.*

2.8 Die Sylowsätze

Definition 2.25. Sei G eine endliche Gruppe und p ein Primteiler von $|G|$. Eine Untergruppe von G heißt *p-Sylowgruppe* von G falls ihre Ordnung die höchste p-Potenz ist, die $|G|$ teilt.

Eine p-Sylowgruppe ist also eine maximale p-Untergruppe von G. Für $p \nmid |G|$ ist offenbar die triviale Gruppe eine p-Sylowgruppe von G.

Beispiel 2.8.1. *1. $P = \{(1), (123), (132)\}$ ist eine 3-Sylowgruppe von S_4.*

2. $P = \{(1), (1234), (13)(24), (1432), (24), (14)(23), (13), (12)(34)\}$ ist eine 2-Sylowgruppe von S_4. Sie ist isomorph zu D_4.

Hier haben wir $|S_4| = 24 = 2^3 \cdot 3$, und $r = (1234)$, $s = (24)$ für D_4.

Für die Sylowsätze benötigen wir folgendes Lemma.

Lemma 2.8.2. *Sei H eine p-Gruppe, die auf einer endlichen Menge X operiert und sei X^H die Menge der Punkte, die von H fixiert wird, d.h.*

$$X^H = \{x \in X \mid hx = x \; \forall\, h \in H\}.$$

Dann gilt

$$|X| \equiv |X^H| \bmod p.$$

Insbesondere folgt

$$|H| \equiv |Z(H)| \bmod p.$$

Beweis. Es gilt $(H : \mathrm{Stab}(x_0)) = |Hx_0|$ wegen Theorem 2.7.1. Da H eine p-Gruppe ist, muss dieser Index eine p-Potenz sein. Also besteht Hx_0 entweder nur aus einem Element, oder $|Hx_0|$ ist durch p teilbar. Da X die disjunkte Vereinigung seiner Bahnen ist, folgt die erste Behauptung. Wendet man diese auf die Konjugationsoperation an, so erhält man die zweite Behauptung. □

Theorem 2.8.3 (Sylow I)**.** *Sei G eine endliche Gruppe und p eine Primzahl. Gilt $p^r \mid |G|$ für ein $r \geq 1$, dann hat G eine Untergruppe der Ordnung p^r.*

Beweis. Wegen Satz 2.7.12 genügt es die Aussage für den Fall zu beweisen, wo $p^r \,||\, |G|$ die höchste p-Potenz ist, die $|G|$ teilt. Denn wenn G eine Untergruppe der Ordnung p^r hat, so hat sie auch Untergruppen aller möglichen kleineren Ordnungen $1, p, p^2, \ldots, p^r$. Wir können also annehmen, dass $|G| = p^r m$ mit $p \nmid m$ ist. Sei

$$X = \{S \subseteq G \mid |S| = p^r\}.$$

Definiere eine G-Operation auf X durch

$$(g, A) \mapsto gA = \{ga \mid a \in A\}.$$

Sei $A \in X$, i.e., $A = \{g_1, \ldots, g_{p^r}\}$ und sei

$$H = \mathrm{Stab}(A) = \{g \in G \mid gA = A\}.$$

Für jedes $g_i \in A$ ist die Abbildung $h \mapsto hg_i$, $H \to A$ injektiv wegen des Kürzungsgesetzes, und so gilt

$$(H : 1) \leq |A| = p^r.$$

In der Gleichung

$$(G : 1) = (G : H)(H : 1)$$

ist $(G : 1) = p^r m$ mit $p \nmid m$ und $(H : 1) = p^k$ mit $k \leq r$, und $(G : H)$ ist die Anzahl der Elemente in dem Orbit von A. Also genügt es, eine *einzige* Menge A zu finden, für die p nicht die Anzahl der Elemente in ihrer Bahn teilt. Denn dann können wir, für dieses spezielle A, schliessen, dass die Untergruppe $H = \mathrm{Stab}(A)$ Ordnung p^r hat, und wir sind fertig. Die Anzahl der Elemente in X ist

$$|X| = \binom{p^r m}{p^r} = \frac{(p^r m)(p^r m - 1) \cdots (p^r m - i) \cdots (p^r m - p^r + 1)}{p^r (p^r - 1) \cdots (p^r - i) \cdots (p^r - p^r + 1)}.$$

Wegen $i < p^r$ ist die p-Potenz, die $p^r m - i$ teilt gleich der p-Potenz, die i teilt. Das gleiche gilt für $p^r - i$. Also sind die entsprechenden Terme über und unter dem Bruchstrich durch die gleiche p-Potenz teilbar, so dass p *kein Teiler* von $|X|$ ist. Da die Bahnen eine Partition von X bilden, muss mindestens eine Bahn (für eine Menge A) nicht durch p teilbar sein. Das zeigt die Behauptung. □

Korollar 2.8.4. *Für p-Gruppen gilt die Umkehrung des Theorems von Lagrange. Für jeden Teiler $d \mid |G|$ gibt es eine Untergruppe der Ordnung d.*

Im allgemeinen gilt die Umkehrung von Lagrange nicht. Die Gruppe A_4 hat Ordnung 12, und $d = 6$ ist ein Teiler von 12. Es gibt aber keine Untergruppe der Ordnung 6 von A_4:

Beispiel 2.8.5. *Die Untergruppen von A_4 sind wie folgt gegeben:*

Ordnung	#	*Untergruppen*
1	1	$\{(1)\}$
2	3	$\{(1),(12)(34)\}$, $\{(1),(13)(24)\}$, $\{(1),(14)(23)\}$
3	4	$\{(1),(123),(132)\}$, $\{(1),(243),(234)\}$, $\{(1),(142),(124)\}$, $\{(1),(134),(143)\}$
4	1	$\{(1),(12)(34),(13)(24),(14)(23)\}$
12	1	$\{(1),(12)(34),(13)(24),(14)(23),(123),(243),(142),(134),(132),(143),(234),(124)\}$

Nach Sylow I gibt es Untergruppen der Ordnung 2, 2^2, und 3. Die Gruppe der Ordnung 4 ist die eindeutige 2-Sylowgruppe von A_4, und die vier Gruppen der Ordnung 3 sind die 3-Sylowgruppen von A_4.

Bemerkung 2.8.6. Sylow I impliziert den Satz von Cauchy. Gilt $p \mid |G|$, so hat G eine Untergruppe H der Ordnung p. Dann hat jedes Element $h \in H$ außer e die Ordnung p.

Lemma 2.8.7. *Sei P eine p-Sylowgruppe von G und H eine p-Untergruppe. Falls H die p-Sylowgruppe P normalisiert, d.h., falls $H \subseteq N_G(P)$ gilt, dann folgt $H \subseteq P$. Insbesondere normalisiert P keine andere p-Sylowgruppe von G ausser sich selbst.*

Beweis. Da H und P Untergruppen von $N_G(P)$ sind, und P normal in $N_G(P)$, ist HP eine Untergruppe. Der zweite Isomorphiesatz gibt

$$H/H \cap P \cong HP/P.$$

Daher ist $(HP : P)$ eine p-Potenz, denn $(H : 1)$ ist eine p-Potenz nach Voraussetzung. Wir haben aber

$$(HP : 1) = (HP : P)(P : 1),$$

und $(P : 1)$ ist die größte p-Potenz, die $(G : 1)$ teilt, also auch die größte p-Potenz, die $(HP : 1)$ teilt. Also gilt $(HP : P) = p^0 = 1$ und $H \subseteq P$. □

Theorem 2.8.8 (Sylow II)**.** *Je zwei p-Sylowgruppen von G sind konjugiert, also isomorph.*

Beweis. Sei X die Menge der p-Sylowgruppen in G, und operiere G auf X durch Konjugation, d.h., durch

$$(g, P) \mapsto gPg^{-1}.$$

Sei O eine der G-Bahnen. Wir wollen $O = X$ zeigen. Sei $P \in O$ und P operiere durch die Aktion von G. Die G-Bahn O spaltet sich unter dieser Operation auf in mehrere P-Bahnen, wovon eine P sein wird. Das muss auch die *einzige* einelementige Bahn sein, da $\{Q\}$ genau dann eine P-Bahn ist, wenn P das Q normalisiert. Das passiert wegen Lemma 2.8.7 aber nur für $Q = P$. Also ist die Anzahl der Elemente in jeder P-Bahn, die verschieden von $\{P\}$ ist, durch p teilbar und wir haben

$$|O| \equiv 1 \bmod p.$$

Angenommen es gibt eine p-Sylowgruppe P, die nicht in X liegt. Dann zeigt das vorangegangene Argument, dass die Anzahl der Elemente in jeder P-Bahn durch p teilbar ist, da es keine einelementigen Bahnen gibt in diesem Fall. Also erhalten wir $|O| \equiv 0 \bmod p$, einen Widerspruch. Also gibt es kein P mit $P \notin O$, und es folgt $O = X$. □

Theorem 2.8.9 (Sylow III)**.** *Sei s_p die Anzahl der p-Sylowgruppen in G und sei $|G| = p^r m$ mit $p \nmid m$. Dann gilt $s_p \mid m$, und $s_p = (G : N_G(P))$ für jede p-Sylowgruppe P of G. Wir haben*

$$s_p \equiv 1 \bmod p.$$

Beweis. Im Beweis von Sylow II haben wir schon gezeigt, dass $s_p = |O| \equiv 1 \bmod p$. Sei P eine p-Sylowgruppe von G. In Korollar 2.7.2 haben wir gezeigt, dass die Anzahl der Konjugierten von P durch $(G : N_G(H))$ gegeben ist. Aber das ist gerade s_p. Weiterhin gilt

$$\begin{aligned}(G : N_G(P)) &= \frac{(G:1)}{(N_G(P):1)} \\ &= \frac{(G:1)}{(N_G(P):P)(P:1)} \\ &= \frac{m}{(N_G(P):P)},\end{aligned}$$

welches ein Faktor von m ist. Also hat man $s_p \mid m$. □

Korollar 2.8.10. *Jede p-Untergruppe von G ist in einer p-Sylowgruppe enthalten.*

Beweis. Sei H eine p-Untergruppe von G und operiere H auf der Menge X der p-Sylowgruppen von G durch Konjugation. Da $|X| = s_p$ nicht durch p teilbar ist wegen Sylow III, muss X^H nicht-leer sein wegen Lemma 2.8.2. Das bedeutet, es gibt mindestens eine H-Bahn, die aus einer einzigen p-Sylowgruppe besteht. Aber dann normalisiert H die Gruppe P und Lemma 2.8.7 impliziert $H \subseteq P$. □

Korollar 2.8.11. *Eine p-Sylowgruppe von G ist genau dann normal, wenn sie die einzige p-Sylowgruppe ist.*

Beweis. Angenommen, P ist normal. Dann ist P wegen Sylow II die einzige p-Sylowgruppe, denn jede andere p-Sylowgruppe Q erfüllt $Q = gPg^{-1} = P$. Umgekeht sei $s_p = 1$. Dann ist $gPg^{-1} = P$, so dass P normal ist. □

Korollar 2.8.12. *Angenommen G hat nur eine einzige p-Sylowgruppe für jede Primzahl p mit $p \mid |G|$. Dann ist G das direkte Produkt seiner p-Sylowgruppen.*

Beweis. Es seien $P_1, \ldots, P_k$ die Sylowgruppen von G. Es gilt $|P_i| = p_i^{r_i}$ mit verschiedenen Primzahlen p_i, die $|G|$ teilen. Wegen Korollar 2.8.11 ist jedes P_i normal in G, so dass das Produkt $P_1 \cdots P_k$ ebenfalls normal in G ist. Mit Induktion über k folgt nun, dass $|P_1 \cdots P_k| = p_1^{r_1} \cdots p_k^{r_k}$ gilt. Für $k = 1$ gibt es nichts zu zeigen, so dass wir $k \geq 2$ und $|P_1 \cdots P_{k-1}| = p_1^{r_1} \cdots p_{k-1}^{r_{k-1}}$ annehmen können. Dann ist $P_1 \cdots P_{k-1} \cap P_k = 1$, so dass $(P_1 \cdots P_{k-1})P_k$ das direkte Product von $P_1 \cdots P_{k-1}$ und P_k ist, und daher Ordnung $p_1^{r_1} \cdots p_k^{r_k}$ hat. Nun ist G das direkte Produkt seiner p-Sylowgruppen, da G das Produkt von ihnen ist, jede davon normal in G ist, und alle Schnitte $P_j \cap (P_1 \cdots P_{j-1} P_{j+1} \cdots P_k)$ trivial sind. □

Dieses Korollar kann man anwenden, um zu zeigen, dass Gruppen gewisser Ordnung abelsch sind.

Beispiel 2.8.13. *Jede Gruppe G der Ordnung 99 ist kommutativ.*

Wir haben $99 = 3^2 \cdot 11$ und $s_{11} \mid 9$, $s_{11} \equiv 1 \bmod 11$. Das bedeutet $s_{11} = 1$. Also gibt es genau eine 11-Sylowgruppe H in G, und sie ist normal in G. Ebenso gilt $s_3 \mid 11$ und $s_3 \equiv 1 \bmod 3$, also $s_3 = 1$. Also gibt es genau eine 3-Sylowgruppe K in G, und sie ist normal in G. Aus Korollar 2.8.12 folgt $G = H \times K$, wo H und K kommutativ sind. Also ist G abeslch.

Bemerkung 2.8.14. Das gleiche Argument zeigt, dass jede Gruppe der Ordnung p^2q mit Primzahlen $p < q$ und $q \not\equiv 1 \bmod p$ kommutativ ist.

Definition 2.26. Eine nicht-triviale Gruppe G heißt *einfach*, falls sie als Normalteiler nur G und die triviale Gruppe $1 = \{e\}$ mit dem neutralen Element e hat.

Gruppen der Ordnung p^n mit $n \geq 2$ sind nicht einfach wegen Satz 2.7.12. Für $n = 1$ sind sie einfach, wegen Lagrange. Die Gruppe $\mathbb{Z}$ ist nicht einfach, da $2\mathbb{Z}$ ein echter Normalteiler ist. Die Gruppe $GL_2(\mathbb{R})$ ist nicht einfach, da $SL_2(\mathbb{R})$ ein echter Normalteiler ist.
Man kann leicht zeigen, dass eine kommutative Gruppe genau dann einfach ist, wenn sie Primzahlordnung hat, also isomorph zu einer zyklischen Gruppe C_p ist. Die kleinste nicht-abelsche einfache Gruppe ist A_5, die Ordnung 60 hat.

Bemerkung 2.8.15. Ein großes Projekt in der Mathematik des 20. Jahrhunderts war die Klassifikation der *endlichen* einfachen (nicht-abelschen) Gruppen. Um die 100 Mathematiker haben hierzu Beiträge geleistet, die zusammmen über 10000 Seiten füllen. Die Klassifikation ist inzwischen abgeschlossen, die letzten Lücken wurden 2004 geschlossen:

Es gibt 18 unendliche *Serien* von einfachen Gruppen, nämlich die zyklischen Gruppen C_p mit $p \in \mathbb{P}$, die alternierenden Gruppen A_n mit $n \geq 5$, und 16 Serien vom Lie-Typ, die komplizierter zu beschreiben sind. Hinzu kommen 26 sogenannte *sporadische* Gruppen,

die in keine dieser Serien passen. Die kleinste dieser sporadischen Gruppen hat Ordnung 7920, die größte wird das *Monster* genannt und hat die Ordnung

$$\begin{aligned}|M| &= 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \\ &\simeq 8 \cdot 10^{53}.\end{aligned}$$

Lemma 2.8.16. *Sei G eine endliche Gruppe und p die kleinste Primzahl, die $|G|$ teilt. Dann ist jede Untergruppe H vom Index p normal in G.*

Beweis. Sei H eine Untergruppe von G mit $(G : H) = p$. G operiere auf der Menge der Linksnebenklassen G/H durch Linksmultiplikation. Diese Aktion ist nicht-trivial, und induziert daher einen nicht-trivialen Gruppenhomomorphismus

$$\theta : G \to \mathrm{Sym}(G/H) = S_p.$$

Da die Aktion transitiv ist, ist $\ker(\theta)$ der größte Normalteiler N von G, der in H enthalten ist. Angenommen, $N \neq H$. Es gilt

$$(G : N) = (G : H)(H : N) = p(H : N).$$

Da wir $(H : N) > 1$ annehmen, existiert eine Primzahl q, die diesen Index teilt. Da p die kleinste Primzahl ist, die $|G|$ teilt, haben wir $p \leq q$. Also gilt

$$pq \mid (G : N) = \frac{|G|}{|N|} = |\mathrm{im}(\theta)| \mid p! = |S_p|.$$

Aber $pq \mid p!$ ist unmögich für $q \geq p$, Widerspruch. Also ist $N = H$, und das ist ein Normalteiler von G. □

Wir können dieses Lemma zusammen mit den Sylowsätzen anwenden, um zu zeigen, daß Gruppen von gewisser Ordnung nicht einfach sein können.

Satz 2.8.17. *Sei G eine Gruppe der Ordung pq^r für Primzahlen $p < q$ mit $r \geq 1$. Dann ist G nicht einfach.*

Beweis. Sei H eine q-Sylowgruppe von G. Wegen Lemma 2.8.16 ist H normal. es gilt $|H| = q^r$, also ist H ein echter Normalteiler. □

Wir erwähnen noch ein berühmtes Resultat von Burnside.

Theorem 2.8.18 (Burnside 1901)**.** *Sei G eine Gruppe der Ordnung $p^r q^s$ für Primzahlen $p < q$ und $r, s \geq 1$. Dann ist G nicht einfach.*

Dieser Satz kann nicht auf Gruppenordnungen mit drei verschiedenen Primzahlen verallgemeinert werden, da $|A_5| = 60 = 2^2 \cdot 3 \cdot 5$, und A_5 einfach ist.

Wir wollen nun noch zeigen, dass nicht nur Gruppen von Primzahlordnung zyklisch sind, sondern auch solche der Ordnung pq mit zwei verschiedenen Primzahlen $p < q$, sofern p nicht $q - 1$ teilt. Dazu benötigen wir zuerst das folgende Lemma.

Lemma 2.8.19. *Sind p und q zwei verschiedene Primteiler von $|G|$ mit $s_p = s_q = 1$, dann kommutieren die Elemente der p-Sylowgruppe mit den Elementen der q-Sylowgruppe.*

Beweis. Sei P die p-Sylowgruppe und Q die q-Sylowgruppe von G. Da die Ordnungen von P und Q relativ prim sind, folgt $P \cap Q = 1$ wegen Lagrange. Die Untergruppen P und Q sind normal in G wegen Korollar 2.8.11. Für $a \in P$ und $b \in Q$ gilt

$$aba^{-1}b^{-1} = (aba^{-1})b^{-1} = a(ba^{-1}b^{-1}) \in P \cap Q = 1,$$

so dass $ab = ba$. □

Satz 2.8.20. *Sei G eine Gruppe der Ordnung pq mit Primzahlen $p < q$ und $q \not\equiv 1 \bmod p$. Dann ist G zyklisch.*

Beweis. Wegen Cauchys Theorem hat G ein Element a der Ordnung p und ein Element b der Ordnung q. Sei $P = \langle a \rangle$ und $Q = \langle b \rangle$. Diese Untergruppen haben Ordnung p und q, und P ist eine p-Sylowgruppe, Q ist eine q-Sylowgruppe. Wegen Sylow III gilt $s_p \mid q$ und $s_p \equiv 1 \bmod p$. Wegen $q \not\equiv 1 \bmod p$ muss $s_p = 1$ gelten, so dass P normal in G ist. Ebenso folgt $s_q \mid p$ und $s_q \equiv 1 \bmod q$. Wegen $1 < p < q$ und $q \not\equiv 1 \bmod p$ muss auch $s_q = 1$ gelten. Daher ist Q normal in G. Nun können wir Lemma 2.8.19 anwenden, um zu zeigen, dass die Elemente von P mit den Elementen von Q kommutieren. Insbesondere kommutieren die Erzeuger a und b, d.h., $ab = ba$, und $\mathrm{ord}(a)$, $\mathrm{ord}(b)$ sind teilerfremd. Deshalb gilt $\mathrm{ord}(ab) = pq$, und ab erzeugt G. □

Zum Beispiel ist $f(n) = 1$ für $n = 15, 33, 35, 51, 65, 69, 77, 85, 87, 91, 95$ mit $n = pq$ und

$$\begin{aligned}(p,q) &= (3,5),(3,11),(5,7),(3,17),(5,13),(3,23),(7,11),\\ &= (5,17),(3,29),(7,13),(5,19).\end{aligned}$$

Das sind alle Beispiele dieser Art für $n < 100$.

Bemerkung 2.8.21. Es gilt $f(n) = 1$ genau dann wenn $\gcd(n, \varphi(n)) = 1$ ist. Das wurde 1947 von von Tibor Szele bewiesen, in der Arbeit *Über die endichen Ordnungszahlen, zu denen nur eine Gruppe gehört*, siehe [8].

2.9 Semidirekte Produkte

Das *semidirekte* Produkt zweier Gruppen N und Q ist eine Verallgemeinerung des direkten Produktes $N \times Q$, unter Verwendung eines Gruppenhomomorphismus $\theta\colon Q \to \mathrm{Aut}(N)$.
Dazu wollen wir zuerst nochmal an die Gruppe $\mathrm{Inn}(G)$ der inneren Automorphismen von G erinnern. Die Elemente sind von der Form i_g, gegeben durch $i_g(x) = gxg^{-1}$.

Lemma 2.9.1. *Sei G eine Gruppe. Dann gilt $G/Z(G) \cong \mathrm{Inn}(G)$.*

Beweis. Die Abbildung $\varphi\colon G \to \mathrm{Aut}(G)$, $g \mapsto i_g$ ist ein Gruppenhomomorphismus mit Kern $Z(G)$. Nach Korollar 2.3.14 gilt $G/\ker(\varphi) \cong \mathrm{im}(\varphi)$. □

Beispiel 2.9.2. *Für die Quaternionengruppe Q_8 gilt* $\mathrm{Inn}(Q_8) \cong C_2 \times C_2$.

In der Tat, wegen $Z(Q_8) = \{\pm 1\}$ gilt $\mathrm{Inn}(Q_8) \cong Q_8/\{\pm 1\} \cong C_2 \times C_2$. Man kann zeigen, dass $\mathrm{Aut}(Q_8) \cong S_4$ gilt.

Lemma 2.9.3. *Die Untergruppe* $\mathrm{Inn}(G)$ *ist normal in* $\mathrm{Aut}(G)$.

Beweis. Sei $g \in G$ und $\alpha \in \mathrm{Aut}(G)$. Dann gilt

$$\begin{aligned}(\alpha \circ i_g \circ \alpha^{-1})(x) &= \alpha(g \cdot \alpha^{-1}(x) \cdot g^{-1}) \\ &= \alpha(g) \cdot x \cdot \alpha(g)^{-1} \\ &= i_{\alpha(g)}(x).\end{aligned}$$

□

Definition 2.27. Sei G eine Gruppe. Die Faktorgruppe

$$\mathrm{Out}(G) = \mathrm{Aut}(G)/Inn(G)$$

wird die *äußere Automorphismengruppe* von G genannt.

Ein wichtiges Problem ist, zu entscheiden wann die Gruppe $\mathrm{Out}(G)$ trivial ist.

Bemerkung 2.9.4. Es gilt $\mathrm{Out}(S_n) = 1$ für alle $n \geq 1$ mit $n \neq 6$.

Kommen wir jetzt zum semidirekten Produkt. Sei N ein Normalteiler von G. Jedes Element $g \in G$ definiert einen Automorphismus von N durch $n \mapsto gng^{-1}$, und das definiert einen Homomorphismus

$$\theta\colon G \to \mathrm{Aut}(N),\ g \mapsto i_{g|N}.$$

Angenommen, es existiert eine Untergruppe Q von G, so dass der kanonische Homomorphismus $\pi\colon G \to G/N$ die Gruppe Q isomorph auf G/N abbildet. Dann können wir G aus dem Tripel $(N, Q, \theta_{|Q})$ rekonstruieren. Jedes $g \in G$ kann nämlich eindeutig in der Form $g = nq$ mit $n \in N$ und $q \in Q$ geschrieben werden, wobei q das eindeutige Element von Q sein muss, dass auf $gN \in G/N$ abgebildet wird, und n gleich gq^{-1} sein muss. Also haben wir eine bijektive Korrespondenz der Mengen

$$G \leftrightarrow N \times Q.$$

Das Produkt zweier Elemente $g = nq$ und $g' = n'q'$ ist wie folgt gegeben,

$$\begin{aligned}gg' &= (nq)(n'q') \\ &= n(qn'q^{-1})qq' \\ &= n \cdot \theta(q)(n') \cdot qq'.\end{aligned}$$

Wir definieren nun das semidirekte Produkt genau nach dieser obigen Annahme.

Definition 2.28. Eine Gruppe G ist das *semidirekte Produkt* seiner Untergruppen N und Q, falls N ein Normalteiler ist und $G \to G/N$ einen Isomorphismus $Q \to G/N$ induziert. Wir schreiben dann $G = N \rtimes Q$.

Wir schreiben oft auch genauer $G = N \rtimes_\theta Q$, wobei $\theta\colon Q \to \mathrm{Aut}(N)$ die Operation von Q auf N durch innere Automorphismen ergibt. Man beachte, dass Q kein Normalteiler von G sein muss.

Bemerkung 2.9.5. Es ist leicht zu zeigen, dass G genau dann ein semidirektes Produkt seiner Untergruppen N und Q ist, falls N ein Normalteiler ist, $NQ = G$ und $N \cap Q = 1$ gilt.

Das semidirekte Produkt $N \rtimes_\theta Q$ wird wie folgt aus zwei Gruppen N und Q und einem Homomorphismus $\theta\colon Q \to \mathrm{Aut}(N)$ konstruiert. Es sei $G = N \times Q$ als Menge. Man definiere die Komposition in G durch

$$(n, q)(n', q') = (n \cdot \theta(q)(n'), qq'). \tag{2.1}$$

Satz 2.9.6. *Mit dieser Komposition ist G eine Gruppe, und es gilt $G \cong N \rtimes_\theta Q$.*

Beweis. Wir schreiben ${}^q n$ für $\theta(q)(n)$. Dann gilt

$$\begin{aligned}((n, q)(n', q'))(n'', q'') &= (n \cdot {}^q n' \cdot {}^{qq'} n'', qq'q'') \\ &= (n, q)((n', q')(n'', q'')).\end{aligned}$$

Also gilt das Assoziativgesetz in G. Wegen $\theta(1) = 1$ und ${}^q 1 = 1$ hat man

$$(1, 1)(n, q) = (n, q) = (n, q)(1, 1).$$

Also ist $(1, 1)$ das neutrale Element. Wegen

$$\begin{aligned}(n, q)({}^{q^{-1}} n^{-1}, q^{-1}) &= (1, 1) \\ &= ({}^{q^{-1}} n^{-1}, q^{-1})(n, q),\end{aligned}$$

ist $({}^{q^{-1}} n^{-1}, q^{-1})$ das inverse Element von (n, q). Also ist G eine Gruppe. Es ist nicht schwer zu sehen, dass N ein Normalteiler ist mit $QN = G$ und $N \cap Q = 1$. Also ist $G \cong N \rtimes Q$. betrachtet man N und Q als Untergruppen von G, dann ist die Operation von Q auf N durch θ gegeben. □

Beispiel 2.9.7. 1. *Für D_n mit $n \geq 2$ wählen wir $N = \langle r \rangle = C_n$, $Q = \langle s \rangle = C_2$ und $\theta(s)(r^i) = r^{-i}$, und erhalten*

$$D_n = N \rtimes_\theta Q = C_n \rtimes_\theta C_2.$$

2. *Es gilt $S_n = A_n \rtimes C_2$, da A_n ein Normalteiler vom Index 2 in S_n ist, so dass $Q = \{(12)\}$ isomorph auf S_n/A_n abgebildet wird.*

3. *Die Gruppe C_{p^2}, für p prim, ist kein semidirektes Produkt von nicht-trivialen Untergruppen, da sie nur eine Untergruppe der Ordnung p hat, und $C_p \times C_p$ nicht isomorph zu C_{p^2} ist.*

4. *Man kann auch zeigen, dass Q_8 nicht als semidirektes Produkt von zwei nicht-trivialen Untergruppen geschrieben werden kann.*

Beispiel 2.9.8. *Das direkte Produkt $N \times Q$ ist genau dann ismomorph zum semidirekten Produkt $N \rtimes_\theta Q$, wenn θ der triviale Homomorphismus $Q \to \mathrm{Aut}(N)$ ist, gegeben durch $\theta(q)(n) = n$ für alle $q \in Q, n \in N$.*

Beispiel 2.9.9. *Jede Gruppe der Ordnung 6 ist ein semidirektes Produkt, nämlich $C_6 \cong C_3 \times C_2$ und $S_3 \cong C_3 \rtimes_\theta C_2$.*

Es gibt nämlich nur zwei Homomorphismen $\theta\colon C_2 \to \mathrm{Aut}(C_3) \cong C_2$. Der triviale Homomorphismus ergibt das direkte Produkt $C_3 \times C_2$, und der andere ergibt $C_3 \rtimes_\theta C_2$. Den hatten wir schon im Beispiel 2.9.7 für D_3 gesehen, und es gilt $D_3 \cong S_3$.

2.10 Auflösbare und nilpotente Gruppen

Auflösbare Gruppen spielen bei der Auflösung (daher der Name!) von polynomialen Gleichungen

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 = 0$$

durch Radikale eine zentrale Rolle.

Definition 2.29. Sei G eine Gruppe. Eine Kette von absteigenden Untergruppen

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_i \supseteq G_{i+1} \supseteq \cdots \supseteq G_n = 1$$

heißt *Subnormalreihe*, wenn G_i normal in G_{i-1} ist für jedes i. Ist zusätzlich G_i normal in G für alle i, dann heißt sie *Normalreihe* von G.

Die Quotientengruppen G_i/G_{i+1} heißen *Faktoren* der Reihe, und die *Länge* der Reihe ist die Anzahl der strkten Inklusionen. Wir schreiben auch

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_i \rhd G_{i+1} \rhd \cdots \rhd G_n = 1$$

für eine Subnormalreihe, oder

$$1 = G_0 \lhd G_1 \lhd \cdots \lhd G_j \lhd G_{j+1} \lhd \cdots \lhd G_n = G.$$

als aufsteigende Reihe.

Definition 2.30. Eine Subnormalreihe von G heißt *Kompositionsreihe*, wenn alle Quotienten nicht-trivial und einfach sind.

Mit anderen Worten, eine Subnormalreihe ist eine Kompositionsreihe, falls sie keine echte *Verfeinerung* hat, die auch eine Subnormalreihe ist. Verfeinerung bedeutet hier, dass jede Untergruppe der ersten Reihe auch als Term in der zweiten (verfeinerten) Reihe vorkommt. Jede endliche Gruppe besitzt eine Kompositionsreihe.

Beispiel 2.10.1. *Die symmetrische Gruppe S_3 hat eine Kompositionsreihe*

$$S_3 \triangleright A_3 \triangleright 1$$

mit einfachen Faktoren C_2 und C_3.

Definition 2.31. Eine Gruppe G heißt *auflösbar*, falls sie eine Subnormalreihe mit abelschen Faktorgruppen hat.

In diesem Fall nennt man diese Reihe auch *auflösbare Reihe*. Zum Beispiel ist die Gruppe S_3 auflösbar, siehe oben.

Beispiel 2.10.2. *Jede abelsche Gruppe ist auflösbar.*

Beispiel 2.10.3. *Die Gruppe S_4 hat eine Kompositionsreihe*

$$S_4 \triangleright A_4 \triangleright V_4 \triangleright \langle (12)(34) \rangle \triangleright 1,$$

wobei $V_4 \cong C_2 \times C_2$ aus $\{(1), (12)(34), (13)(24), (14)(23)\}$ besteht. Die Faktoren sind C_2, C_3, C_2, C_2, also abelsch. Somit ist S_4 auflösbar.

In der Tat sind die Gruppen S_n für $n \leq 4$ auflösbar, aber nicht auflösbar für alle $n \geq 5$. Das wurde zuerst von Galois gezeigt.

Theorem 2.10.4. *(Galois) Die Gruppe A_n ist einfach für jedes $n \geq 5$.*

Beweis. Die Beweisidee ist wie folgt. Man kann zeigen, dass jeder nicht-triviale Normalteiler N von A_n einen 3-Zykel enthält für $n \geq 5$, und dann alle 3-Zykel enthält. Da wegen Lemma 2.4.8 das Erzeugnis aller 3-Zykel schon A_n ist, folgt $N = A_n$. □

Eine einfache Gruppe ist auflösbar genau dann wenn sie abelsch ist. Die Gruppe A_n für $n \geq 5$ ist also nicht auflösbar, da sie einfach und nicht-abelsch ist.

Korollar 2.10.5. *Die einzigen Normalteiler von S_n für $n \geq 5$ sind $1, A_n$ and S_n. Insbesondere ist S_n nicht auflösbar für $n \geq 5$.*

Beweis. Sei N ein Normalteiler in S_n. Dann ist auch $N \cap A_n$ ein Normalteiler in A_n. Da A_n aber einfach ist, gilt entweder $N \cap A_n = A_n$ oder $N \cap A_n = 1$. Im ersten Fall gilt $N \supseteq A_n$. Da A_n Index 2 in S_n hat, folgt $N = A_n$ oder $N = S_n$. Im Fall $N \cap A_n = 1$ ist die Abbildung $n \mapsto nA_n$ von N nach $S_n/A_n \cong C_2$ injektiv, so dass N die Ordnung 1 oder 2 hat. Aber N kann nicht Ordnung 2 haben, da keine Konjugationsklasse in S_n außer $\{1\}$ aus einem einzigen Element bestehen kann, und N ja die disjunkte Vereinigung aller Konjugationsklassen ist, die triviale Konjugationsklasse eingeschlossen. Somit hat S_n, $n \geq 5$ nur eine einzige Kompositionsreihe, nämlich

$$S_n \triangleright A_n \triangleright 1.$$

Ihre Faktoren sind C_2 und die nicht-abelsche Gruppe A_n. □

Satz 2.10.6. *Jede Untergruppe und jede Quotientengruppe einer auflösbaren Gruppe ist auflösbar.*

Beweis. Sei $G \triangleright G_1 \triangleright \cdots \triangleright G_n$ eine auflösbare Reihe für G und H eine Untergruppe von G. Der Homomorphismus $H \cap G_i \to G_i/G_{i+1}$ mit $x \mapsto xG_{i+1}$ hat den Kern

$$(H \cap G_i) \cap G_{i+1} = H \cap G_{i+1}.$$

Deshalb ist $H \cap G_{i+1}$ ein Normalteiler von $H \cap G_i$ und der Quotient

$$(H \cap G_i)/(H \cap G_{i+1})$$

ist abelsch, weil er injektiv in die abelsche Gruppe G_i/G_{i+1} abgebildet wird. Insgesamt folgt, dass

$$H \triangleright (H \cap G_1) \triangleright \cdots \triangleright (H \cap G_n)$$

eine auflösbare Reihe für H ist.

Sei N ein Normalteiler von G. Wir konstruieren nun eine auflösbare Reihe für G/N aus der auflösbaren Reihe von G. Es gilt $NG_i \triangleright NG_{i+1}$, da N und G_{i+1} beide NG_i normaliseren in G. Also erhalten wir die Normalreihe

$$G = NG_0 \triangleright NG_1 \triangleright \cdots \triangleright NG_n = N.$$

Reduktion modulo N ergibt

$$\overline{G} = G/N \triangleright \overline{G}_1 \triangleright \cdots \triangleright \overline{G}_n = \{\overline{1}\}$$

mit $\overline{G}_i = (NG_i)/N \cong G_i/(N \cap G_i)$. Die natürliche Abbildung $G_i \to \overline{G}_i$ ist surjektiv. Also ist auch $G_i \to \overline{G}_i/\overline{G}_{i+1}$ surjektiv und Null auf G_{i+1}, so dass $\overline{G}_i/\overline{G}_{i+1}$ eine Quotientengruppe von G_i/G_{i+1} ist für alle i, also ebenfalls abelsch ist. Damit haben wir gezeigt, dass die obige Normalreihe eine auflösbare Reihe für G/N ist. □

Satz 2.10.7. *Sei N ein Normalteiler von G und seien N und G/N auflösbar. Dann ist G auflösbar.*

Beweis. Sei $\overline{G} = G/N$ und seien

$$\overline{G} \triangleright \overline{G}_1 \triangleright \cdots \triangleright \overline{G}_n = 1,$$
$$N \triangleright N_1 \triangleright \cdots \triangleright N_m = 1$$

auflösbaren Reihen für $\overline{G}$ bzw. N. Sei G_i das inverse Bild von $\overline{G}_i$ in G, d.h., mit $G_i \mapsto \overline{G_i}$ unter der Quotientenabbildung $G \to G/N$. Dann gilt

$$G_i/G_{i+1} \cong \overline{G}_i/\overline{G}_{i+1},$$

und somit ist

$$G \triangleright G_1 \triangleright \cdots \triangleright (G_n = N) \triangleright N_1 \triangleright \cdots \triangleright N_m$$

eine auflösbare Reihe für G. □

Korollar 2.10.8. *Jede p-Gruppe ist auflösbar.*

Beweis. Sei G eine nicht-triviale p-Gruppe. Wir zeigen die Behauptung mit Induktion über $|G|$. Da $Z(G)$ nicht-trivial ist wegen Satz 2.7.11, ist $G/Z(G)$ auflösbar nach Induktionsannahme. Da $Z(G)$ abelsch und somit auflösbar ist, ist wegen Satz 2.10.7 auch G auflösbar. □

Für eine auflösbare Gruppe G gibt es eine *kanonische* auflösbare Reihe, nämlich die *abgeleitete Reihe*. Das ist übrigens die kürzeste auflösbare Reihe für G. Der *Kommutator* von zwei Elementen x, y in G ist definiert als

$$[x, y] := xyx^{-1}y^{-1} = (xy)(yx)^{-1}.$$

Also bedeutet $[x, y] = e$, dass x und y kommutieren, d.h., $xy = yx$.

Definition 2.32. Sei G eine Gruppe. Die *abgeleitete Gruppe*, oder auch die *Kommutatoruntergruppe* von G ist die Gruppe, die von allen Kommutatoren von G erzeugt wird. Sie wird mit G' bzw. $[G, G]$ bezeichnet.

Man beachte, dass G' nicht nur aus Kommutatoren bestehen muss. Sie ist nur *erzeugt* von allen Kommutatoren.

Definition 2.33. Eine Untergruppe H von G heißt *charakteristisch*, falls $\varphi(H) \subseteq H$ für alle $\varphi \in \mathrm{Aut}(G)$ gilt.

Lemma 2.10.9. *Die Kommutatoruntergruppe von G ist eine charakteristische Untergruppe von G, und daher auch ein Normalteiler von G.*

Beweis. Seien x, y in G und $\varphi \in \mathrm{Aut}(G)$. Dann gilt

$$\begin{aligned}\varphi([x, y]) &= \varphi(xyx^{-1}y^{-1}) \\ &= \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} \\ &= [\varphi(x), \varphi(y)].\end{aligned}$$

Also werden die Erzeuger von G' auf G' abgebildet. Deshalb folgt $\varphi(G') \subseteq G'$ für alle Automorphismen von G. Betrachtet man die inneren Automorphismen, so folgt $gG'g^{-1} \subseteq G'$ für alle $g \in G$. Also ist G' ein Normalteiler von G. □

Beispiel 2.10.10. 1. *Eine Gruppe G ist abelsch genau dann wenn $G' = 1$.*

2. *Für $n \geq 3$ gilt $D_n' = \langle r^2 \rangle$, mit $[r, s] = r(sr^{-1}s^{-1}) = r^2$.*

3. *Für $n \geq 5$ gilt $A_n' = A_n$, da $[(abd), (ace)] = (abc)$ für verschiedene a, b, c, d, e, und da A_n von allen 3-Zykeln erzeugt wird.*

4. *Es gilt $A_4' = V_4$, welches die normale 2-Sylowgruppe von A_4 ist.*

5. *Es gilt $Q_8' = \{\pm 1\} = Z(Q_8)$.*

Satz 2.10.11. *Die Kommutatoruntergruppe G' ist der kleinste Normalteiler N von G, so dass G/N abelsch ist.*

Beweis. Wir zeigen zuerst, dass G/G' abelsch ist. Der kanonische Homomorphismus $\pi\colon G \to G/G'$ bildet g auf $\overline{g} = gG'$ ab. Es gilt

$$[\overline{g}, \overline{h}] = \overline{[g,h]} = \overline{1}$$

für alle g, h, wegen $[g,h] \in G'$. Also kommutieren alle $\overline{g}, \overline{h}$ in G/G'.
Sei N ein Normalteiler von G mit G/N abelsch. Dann ist das Bild von $[g,h]$ in G/N wieder trivial, so dass $[g,h] \in N$. Da diese Elemente G' erzeugen, gilt $N \supseteq G'$. □

Beispiel 2.10.12. *Für $n \geq 5$ gilt $S_n' = A_n$, da A_n der kleinste Normalteiler von S_n mit abelschem Quotient ist.*

Definition 2.34. Die *abgeleitete Reihe* von G ist gegeben durch

$$G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \cdots$$

mit $G^{(i+1)} = [G^{(i)}, G^{(i)}] = (G^{(i)})'$ für alle i.

Wir haben $G = G^{(0)}$, $G' = G^{(1)} = [G,G]$, $G'' = G^{(2)} = [[G,G],[G,G]]$ und so weiter.

Beispiel 2.10.13. *Die abgeleitete Reihe von S_n für $n \geq 5$ ist*

$$S_n \triangleright A_n \trianglerighteq A_n \trianglerighteq \cdots$$

und endet nicht mit der trivialen Gruppe.

Es stellt sich heraus, dass eine Gruppe G genau dann auflösbar ist, wenn ihre abgeleitete Reihe mit der trivialen Gruppe endet.

Satz 2.10.14. *Eine Gruppe G ist genau dann auflösbar, wenn $G^{(s)} = 1$ für ein $s \geq 0$ gilt.*

Beweis. Gilt $G^{(s)} = 1$, dann ist die abgeleitete Reihe natürlich eine auflösbare Reihe für G. Sei umgekehrt

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_s = 1$$

eine auflösbare Reihe für G. Da G/G_1 abelsch ist, gilt $G_1 \supseteq G'$ nach Satz 2.10.11. Nun ist $G'G_2$ eine Untergruppe von G_1, und wegen

$$G'/(G' \cap G_2) \cong G'G_2/G_2 \subseteq G_1/G_2$$

sehen wir, dass die Kommutativität von G_1/G_2 die von $G'/(G' \cap G_2)$ impliziert. Das bedeutet aber $G'' \subset G' \cap G_2 \subseteq G_2$. Fahren wir in dieser Weise fort, folgt $G^{(i)} \subseteq G_i$ für alle i, und deshalb $G^{(s)} = 1$. □

Der zweite Teil des Beweises zeigt auch, dass die abgeleitete Reihe einer auflösbaren Gruppe die kürzeste auflösbare Reihe ist.

Definition 2.35. Das kleinste $i \geq 0$ mit $G^{(i)} = 1$, beziehungsweise die Anzahl der Faktoren in der abgeleiteten Reihe von G heißt die *Auflösbarkeitsklasse*, oder *abgeleitete Länge* von G.

Beispiel 2.10.15. 1. *Für $n \geq 3$ ist D_n auflösbar der Klasse 2, mit abgeleiteter Reihe* $D_n \triangleright \langle r^2 \rangle \triangleright 1$.

2. *S_4 ist auflösbar der Klasse 3, mit* $S_4 \triangleright A_4 \triangleright V_4 \triangleright 1$.

3. *Q_8 ist auflösbar der Klasse 2, mit* $Q_8 \triangleright \{\pm 1\} \triangleright 1$.

Satz 2.10.16. *Sei G eine Gruppe der Ordnung pq mit verschiedenen Primzahlen p und q. Dann ist G auflösbar.*

Beweis. Wegen Sylow III gilt für die Anzahl n_p der p-Sylowgruppen $n_p \equiv 1 \bmod p$ und $n_p \mid q$. Daraus folgt $n_p = 1$, so dass G eine eindeutige p-Sylowgruppe P hat, die deshalb Normalteiler von G ist. Also hat G die auflösbare Reihe $G \triangleright P \triangleright 1$, mit den zyklischen Faktoren $G/P \cong C_q$ und $P \cong C_p$. □

Bemerkung 2.10.17. Burnside zeigte 1904, dass alle Gruppen der Ordnung $p^a q^b$ für Primzahlen $p < q$ und alle $a, b \in \mathbb{N}$ auflösbar sind. Feit und Thompson bewiesen 1963 sogar, dass *alle Gruppen ungerader Ordnung* auflösbar sind. Der Beweis ist 255 Seiten lang und füllt einen kompletten Band des Pacific Journal of Mathematics.

Eine spezielle Klasse auflösbarer Gruppen ist durch *nilpotente* Gruppen gegeben.

Definition 2.36. Eine aufsteigende Reihe von Untergrupppen

$$1 = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_n = G$$

heißt *aufsteigende Zentralreihe* für G, falls $G_i \trianglelefteq G$ und $G_{i+1}/G_i \subseteq Z(G/G_i)$ gilt für alle i. Eine absteigende Reihe

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n = 1$$

heißt *absteigende Zentralreihe*, falls $G_i \trianglelefteq G$ und $G_i/G_{i+1} \subseteq Z(G/G_{i+1})$ gilt für alle i.

Die Bedingung $G_i \trianglelefteq G$ is nötig, damit die Faktorgruppe G/G_i Sinn macht. Es impliziert auch, dass G_i normal in G_{i+1} ist für alle i.

Definition 2.37. Die aufsteigende Reihe

$$1 \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \cdots,$$

wobei $Z_1(G) = Z(G)$ und $Z_i(G)$ rekursiv durch

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$$

definiert ist für alle $i \geq 0$, heißt *obere Zentralreihe* für G, wenn sie mit G endet.
Die absteigende Reihe

$$G^0 = G \supseteq G^1 \supseteq G^2 \supseteq \cdots$$

definiert durch $G^0 = G$ und $G^{i+1} = [G, G_i] = [G_i, G]$ für alle $i \geq 0$, heißt *untere Zentralreihe* für G, wenn sie mit der trivialen Gruppe endet.

Man kann nachprüfen, dass beide Reihen Zentralreihen sind, sofern sie terminieren. Auch das folgende Lemma ist nicht schwer zu zeigen.

Satz 2.10.18. *Für eine Gruppe G sind die folgenden Bedingungen äquivalent:*

(1) $G^c = 1$ *für ein* $c \geq 0$.

(2) $Z_c(G) = G$ *für ein* $c \geq 0$.

(3) G *hat eine Zentralreihe.*

Man beachte dass $G^c = 1$ genau dann gilt wenn $Z_c(G) = G$.

Definition 2.38. Eine Gruppe G heißt *nilpotent*, falls sie eine der drei Bedingungen aus Satz 2.10.18 erfüllt. Die kleinste Zahl $c \geq 0$ mit $G^c = 1$ bzw. $Z_c(G) = G$ heißt dann *Nilpotentzklasse* von G.

Eine Gruppe hat Nilpotenzklasse 0 genau dann, wenn sie trivial ist, und Nilpotenzklasse 1 genau dann, wenn sie abelsch ist und nicht-trivial. G ist nilpotent der Klasse 2 genau dann, wenn $G/Z(G)$ abelsch und nicht-trivial ist.

Korollar 2.10.19. *Sei G eine nicht-triviale nilpotente Gruppe. Dann ist $Z(G)$ nicht-trivial.*

Beweis. Falls $Z(G) = 1$ gilt, so gibt es kein $c \geq 0$ mit $Z_c(G) = G$. Das ist ein Widerspruch zu Satz 2.10.18. □

Beispiel 2.10.20. *Die Gruppe S_3 ist auflösbar, aber nicht nilpotent.*

Es gilt $Z(S_3) = 1$, also kann S_3 nicht nilpotent sein.

Satz 2.10.21. *Jede nilpotente Gruppe ist auflösbar.*

Beweis. Es gilt $G^{(i)} \leq G^i$ für alle $i \geq 0$. Also impliziert $G^c = 1$ auch $G^c = 1$. □

Umgekehrt gibt es Gruppen, die auflösbar sind, aber nicht nilpotent, wie wir mit $S_3 \cong D_3$ bereits gesehen haben. Diedergruppen liefern weitere solche Beispiele.

Beispiel 2.10.22. *Sei $n \geq 3$* ungerade. *Dann ist D_n auflösbar, aber nicht nilpotent.*

Für ungerades $n \geq 3$ gilt $D_n^i = \langle r \rangle$ für alle $i \geq 3$. Also gibt es kein $c \geq 0$ mit $D_n^c = 1$. Diedergruppen können auch für gerade n nilpotent sein.

Bemerkung 2.10.23. Die Diedergruppe D_n ist für $n \geq 3$ genau dann nilpotent, wenn $n = 2^m$ für ein $m \geq 2$ gilt.

Satz 2.10.24. *Jede Gruppe der Ordnung p^3 für p prim ist nilpotent der Klasse $c \leq 2$.*

Beweis. Ist G abelsch, so gilt $c = 1$. Ist G nicht-abelsch, so kann $Z(G)$ nicht Ordnung p^2 haben, da sonst $G/Z(G)$ Ordnung p hätte, also zyklisch wäre und somit G abelsch, nach Lemma 2.7.13. Also gilt $|Z(G)| = p$ wegen $|Z(G)| \neq 1$. Nun ist $|G/Z(G)| = p^2$, weswegen $G/Z(G)$ abelsch ist nach Satz 2.7.14. Aus Satz 2.10.11 folgt $G' \subseteq Z(G)$. Wegen $Z(G) \subseteq G'$ folgt $G' = Z(G)$, und daher $G'' = 1$. □

Insbesondere sind die Gruppen $Q_8, D_4, \mathrm{Heis}(\mathbb{Z}/(p))$ und $\Gamma(p)$ nilpotent der Klasse 2. Wir zeigen nun, dass p-Gruppen immer nilpotent sind.

Satz 2.10.25. *Jede p-Gruppe ist nilpotent.*

Beweis. Sei $|G| = p^n$. Wir führen den Beweis mit Induktion über n. Für $n = 0$ ist G trivial, also nilpotent. Für nicht-triviales G ist auch $Z(G)$ nicht-trivial wegen Korollar 2.10.19. Also ist $G/Z(G)$ eine p-Gruppe kleinerer Ordnung. Nach Induktionsvoraussetzung ist sie nilpotent, d.h.,

$$(G/Z(G))^c = 1$$

für ein c. Sei π der kanonische Homomorphismus $\pi\colon G \to G/Z(G)$. Da π surjektiv ist, gilt

$$\pi(G^c) = (G/Z(G))^c = 1.$$

Also ist $G^c \leq \ker(\pi) = Z(G)$, und somit

$$G^{c+1} = [G^c, G] \leq [Z(G), G] = 1.$$

□

3 Ringe

3.1 Ringaxiome

Definition 3.1. Ein *Ring* R ist eine Menge zusammen mit zwei Abbildungen $+, \cdot \colon R \times R \to R$, genannt Addition und Multiplikation, mit folgenden Eigenschaften.

(1) Das Paar $(R, +)$ bildet eine abelsche Gruppe. Das neutrale Element wird mit 0 bezeichnet, und das additive Inverse zu a mit $-a$.

(2) Die Multiplikation ist assoziativ und es gibt ein Einselement $1 = 1_R$ bezüglich Multiplikation mit $1 \cdot a = a \cdot 1 = a$ für alle $a \in R$.

(3) Es gilt das *Distributivgesetz*, d.h. für alle $a, b, c \in R$ gilt

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$
$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

Gilt weiterhin $a \cdot b = b \cdot a$ für alle $a, b \in R$, so heisst der Ring R *kommutativ*.

Das Axiom (2) kann man auch so formulieren, dass man sagt, $(R, \cdot)$ ist ein *Monoid*. In jedem Ring R gelten die Beziehungen $0 \cdot a = a \cdot 0 = 0$ für alle $a \in R$ und $(-a) \cdot b = a \cdot (-b) = -a \cdot b$ für alle $a, b \in R$. Gilt $1 = 0$, so ist

$$a = a \cdot 1 = a \cdot 0 = 0$$

für alle $a \in R$. Dieser Ring wird als *Nullring* bezeichnet.

Beispiel 3.1.1. 1. *Die Mengen $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ bilden bezüglich der gewöhnlichen Addition und Multiplikation einen kommutativen Ring.*

2. *Die Menge $\mathbb{N}$ bildet bezüglich der gewöhnlichen Addition und Multiplikation keinen Ring, da $(\mathbb{N}, +)$ keine Gruppe ist.*

3. *Die Menge $M_n(K)$ der $n \times n$-Matrizen mit Koeffizienten in einem Körper K bilden einen Ring bezüglich Matrizenaddition und Matrizenmultiplikation. Für $n \geq 2$ ist dieser Ring nicht kommutativ.*

4. *Sind R, S zwei Ringe, so ist deren Produkt $R \times S$, versehen mit der komponentenweisen Addition und Multiplikation, wieder ein Ring.*

5. *Sei $(A, +)$ eine abelsche Gruppe. Dann ist die Menge $\mathrm{End}(A)$ aller Gruppenendomorphismen $\varphi \colon A \to A$ ein Ring, wenn man Summe und Produkt durch*

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x),$$
$$(\varphi \cdot \psi)(x) = \varphi(\psi(x))$$

definiert, für alle $x \in A$, $\varphi, \psi \in \mathrm{End}(A)$.

6. *Ist* K *ein Körper, so ist der Polynomring* $K[X]$ *ein kommutativer Ring.*

Bemerkung 3.1.2. Ein *Körper* ist ein kommutativer Ring K, der nicht der Nullring ist, in dem jedes Element $a \in K^\times$ ein Inverses bezüglich der Multiplikation besitzt. Mit anderen Worten, $(K^\times, \cdot)$ ist eine abelsche Gruppe.

Definition 3.2. Eine Abbildung $\varphi\colon R \to S$ eines Ringes R in einen Ring S heißt *(Ring)homomorphismus*, falls

$$\begin{aligned} \varphi(a+b) &= \varphi(a) + \varphi(b), \\ \varphi(a \cdot b) &= \varphi(a) \cdot \varphi(b), \\ \varphi(1_A) &= 1_B \end{aligned}$$

für alle $a, b \in R$ gilt.

Beispiel 3.1.3. *Die Abbildung*

$$\varphi\colon \mathbb{Z} \to \mathbb{Z},\ \varphi(n) = 2 \cdot n$$

ist kein Ringhomomorphismus, denn die 1 *wird nicht auf die* 1 *abgebildet.*

Verknüpfungen von Ringhomomorphismen sind Ringhomomorphismen und die Identitätsabbildung auf einem Ring ist ein Ringhomomorphismus. Monomorphismus, Endomorphismus, Isomorphismus sind analog definiert, wie bei Gruppen.

Definition 3.3. Eine Teilmenge S eines Ringes R heißt *Unterring* von R, falls S mit den Verknüpfungen $+, \cdot$ von R, eingeschränkt auf S, einen Ring bildet mit $1_S = 1_R$.

Mit anderen Worten, $S \subseteq R$ ist ein Unterring, wenn $1_R \in S$, $a - b \in S$ und $a \cdot b \in S$ für alle $a, b \in S$.

Beispiel 3.1.4. *(Übungsaufgabe)* 1. *Die Menge* $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ *ist ein Unterring von* $\mathbb{C}$. *Er wird der Ring der* Gaußschen ganzen Zahlen *genannt.*

2. *Das* Zentrum $Z(R) = \{x \in R \mid xy = yx \text{ für alle } x, y \in R\}$ *ist ein Unterring von* R.

Der Ring $\mathbb{Z}[i]$ kann zum Beispiel verwendet werden, um zu untersuchen, welche ganzen Zahlen als Summe zweier Quadratzahlen geschrieben werden können. In $\mathbb{Z}[i]$ gilt nämlich für alle $a, b \in \mathbb{Z}$, dass

$$a^2 + b^2 = (a + bi)(a - bi).$$

Eine ungerade Primzahl p kann genau dann als $p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$ dargestellt werden kann, wenn $p \equiv 1 \bmod 4$ gilt (Fermat).

3.2 Ideale und Restklassenringe

Definition 3.4. Eine Teilmenge I eines Ringes R heißt *Linksideal*, falls $(I,+)$ eine Untergruppe von $(R,+)$ ist und $x \cdot a \in I$ für alle $a \in I$ und alle $x \in R$, d.h. $RI \subseteq I$ gilt. Sie heißt *Rechtsideal*, wenn $(I,+) \leq (R,+)$ und $IR \subseteq I$ gilt, und *(beidseitiges) Ideal*, wenn I ein Rechts-und Linksideal ist.

Für kommutative Ring fallen die Begriffe Linksideal, Rechtsideal und beidseitiges Ideal zusammen. Man spricht dann nur von Ideal.

Beispiel 3.2.1. *Sei $R = \mathbb{Z} \times \mathbb{Z}$. Dann ist $S = \{(n,n) \mid n \in \mathbb{Z}\}$ ein Unterring von R, aber kein Ideal.*

Mit $a = (1,1) \in S$ und $x = (1,0) \in R$ gilt $x \cdot a = (1,0) \cdot (1,1) = (1,0) \notin S$. Also ist S kein Ideal.

Beispiel 3.2.2. *Sei $R = M_2(K)$ der Ring der 2×2-Matrizen über einem Körper K. Dann ist*

$$I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in K \right\}$$

ein Linksideal in R, aber kein Rechtsideal, und

$$J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in K \right\}$$

ein Rechtsideal in R, aber kein Linksideal.

Man kann leicht folgendes Resultat zeigen.

Lemma 3.2.3. *Für zwei Ideale I, J in R sind auch folgende Teilmengen*

$$\begin{aligned} I + J &= \{a + b \mid a \in I, b \in J\} \\ IJ &= \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in I, b_i \in J \right\} \\ I \cap J &= \{x \in R \mid x \in I, x \in J\} \end{aligned}$$

wieder Ideale. Es gilt $IJ \subseteq I \cap J$.

Die Summe $I + J$ von zwei Idealen ist das kleinste Ideal von R, das I und J umfasst.

Beispiel 3.2.4. *Sei $R = \mathbb{Z}$ und $I = n\mathbb{Z}$, $J = m\mathbb{Z}$ für $n, m \in \mathbb{Z}$. Dann sind I und J Ideale in R und es bezeichne $(m,n) = \gcd(m,n)$, $[m,n] = \mathrm{lcm}(m,n)$. Dann gilt*

$$\begin{aligned} I + J &= (m,n)\mathbb{Z}, \\ IJ &= (mn)\mathbb{Z}, \\ I \cap J &= [m,n]\mathbb{Z}. \end{aligned}$$

Sei $d = (m, n)$. Wegen $d \mid m$ ist jedes Vielfache von m auch ein Vielfaches von d. Also ist $I \subseteq d\mathbb{Z}$. Ebenso folgt $J \subseteq d\mathbb{Z}$, also $I + J \subseteq d\mathbb{Z}$. Wegen des Euklidischen Algorithmus gibt es $a, b \in \mathbb{Z}$ mit $d = am + bn$. Wegen $am \in I$ und $bn \in J$ folgt $d\mathbb{Z} \subseteq I + J$. Also gilt $I + J = d\mathbb{Z}$.
Die weiteren Behauptungen folgen ebenfalls leicht. Insbesondere gibt es $m, n \in \mathbb{Z}$ mit $IJ \neq I \cap J$.

Satz 3.2.5. *Sei I ein Ideal in $\mathbb{Z}$. Dann gibt es ein $n \in \mathbb{Z}$ mit $I = n\mathbb{Z}$. Für zwei Ideale $m\mathbb{Z}$ und $n\mathbb{Z}$ gilt*

$$m\mathbb{Z} \supseteq n\mathbb{Z} \iff m \mid n.$$

Beweis. Für $I = 0$ ist nichts zu zeigen. Sei also $n \in I$ die kleinste positive Zahl in I. Da I ein Ideal ist, folgt $n\mathbb{Z} \subseteq I$. Ein solches $n \in \mathbb{N}$ existiert, da mit $k \in \mathbb{Z}$ auch $-k \in \mathbb{Z}$ gilt. Sei $a \in \mathbb{Z}$. Dann existieren $q \in \mathbb{Z}$, $r \in \mathbb{N}$ mit

$$a = qn + r,\ 0 \leq r < n.$$

Also ist $r = a - qn \in I$. Da n die kleinste positive Zahl in I war, folgt $r = 0$. Also ist $a = qn$, also $I \subseteq n\mathbb{Z}$. Zusammen folgt $I = n\mathbb{Z}$.
Gilt $n\mathbb{Z} \subseteq m\mathbb{Z}$, so ist $n \in m\mathbb{Z}$, also $n = km$ für ein $k \in \mathbb{Z}$, d.h. $m \mid n$. Gilt umgekehrt $n = km$, und $r \in \mathbb{Z}$, so ist $nr = kmr$, also $n\mathbb{Z} \subseteq m\mathbb{Z}$. □

Satz 3.2.6 (Restklassenring)**.** *Sei R ein Ring und $I \subseteq R$ ein Ideal. Dann ist $R/I = \{x + I \mid x \in R\}$ bezüglich der von der Addition auf R induzierten Addition auf R/I eine abelsche Gruppe. Es gilt:*

(1) *Die Multiplikationsabbildung*

$$R/I \times R/I \to R/I,$$
$$(x + I, y + I) \mapsto (x \cdot y) + I$$

ist wohldefiniert.

(2) *Die Menge R/I bildet bezüglich der obigen Addition bzw. Multiplikation einen Ring, den Restklassenring (Faktorring), von R modulo I.*

Wir schreiben für die Restklassen $x + I$ oft auch kurz $[x]$. Die Abbildung $\pi\colon R \to R/I$, definiert durch $x \mapsto x + I$, ist ein surjektiver Ringhomomorphismus, genannt die *natürliche Projektion.*

Beispiel 3.2.7. *Für $R = \mathbb{Z}$ und $I = n\mathbb{Z}$ erhält man den Faktorring $\mathbb{Z}/n\mathbb{Z}$.*

Die unterliegende additive Gruppe ist die zyklische Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$. Insbesondere enthält $\mathbb{Z}/n\mathbb{Z}$ genau n Elemente: $[0], [1], \ldots, [n-1]$. In diesem Ring gilt, für $n = km$

$$[k] \cdot [m] = [n] = [0].$$

Ist n also zusammengesetzt, so unterscheidet sich die Multiplikation von der bei Körpern. Man hat $[k], [m] \neq [0]$, aber $[k] \cdot [m] = [0]$, sogenannte *Nullteiler.*

Bemerkung 3.2.8. Die Arithmetik in den Restklassenringen der Form $\mathbb{Z}/n\mathbb{Z}$ kann zum Beispiel verwendet werden, um zu zeigen, dass gewisse Gleichungen keine ganzzahligen Lösungen besitzen. Man betrachte etwa die Gleichung

$$x^2 + y^2 = 2019$$

über $\mathbb{Z}$. Angenommen sie hätte eine Lösung in $\mathbb{Z}$. Wir betrachten die kanonische Projektion $\pi\colon \mathbb{Z} \to 4\mathbb{Z}$. Da π ein surjektiver Ringomomorphismus ist, hat die Gleichung auch eine Lösung in $\mathbb{Z}/4\mathbb{Z}$. Jedoch ist $[a^2] = [a]^2$ immer $[0]$ oder $[1]$ in $\mathbb{Z}/4\mathbb{Z}$ und $[2019] = [3]$. Eine Summe aus zwei Restklassen $[0], [1]$ kann aber nur $[0], [1], [2]$ ergeben, ein Widerspruch.

Bemerkung 3.2.9. Die Isomorphiesätze für Gruppen lassen sich analog für Ringe formulieren (und beweisen).

1. Ist $\varphi\colon R \to S$ ein Rinhomomorphismus, so ist $\ker(\varphi)$ ein Ideal in R, $\mathrm{im}(\varphi)$ ein Unterring von S und $R/\ker(\varphi) \cong \mathrm{im}(\varphi)$ für den Faktorring.

2. Sind $S \subseteq R$ ein Unterring von R und I ein Ideal von R, so ist $I + S$ ein Unterring von R, $S \cap I$ ein Ideal von S und $(S + I)/I \cong S/(S \cap I)$.

3. Sind $J \subseteq I$ Ideale in R, dann ist I/J ein Ideal in R/J und $(R/J)/(I/J) \cong R/I$.

3.3 Einheiten, Nullteiler, Integritätsringe

Definition 3.5. Sei R ein Ring. Ein Element $a \in R$ heißt *Einheit* oder *invertierbar*, wenn es ein $b \in R$ gibt mit $ab = ba = 1$. Die Einheiten eines Ringes R bilden eine Gruppe bezüglich Multiplikation, die mit $R^\times$ oder $U(R)$ bezeichnet wird. Sie heißt die *Einheitengruppe* von R.

Man beachte, dass ein Ringisomorphismus einen Gruppenisomorphismus seiner Einheitengruppen induziert.

Beispiel 3.3.1. 1. *Es gilt* $\mathbb{Z}^\times = \{\pm 1\} = C_2$.

2. *Es gilt* $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. *(Übung)*

3. *Es gilt* $(\mathbb{Z}/14\mathbb{Z})^\times = \{[1], [3], [5], [9], [11], [13]\} \cong C_6$.
4. *Die Einheitengruppe des Matrizenringes* $M_n(K)$ *ist die Gruppe* $GL_n(K)$.

Bemerkung 3.3.2. Aus der elementaren Zahlentheorie wissen wir, dass die *prime Restklassengruppe* $(\mathbb{Z}/n\mathbb{Z})^\times$ genau $\varphi(n)$ Elemente hat, und zyklisch ist dann und nur dann, wenn

$$n = 2, 4, p^k, 2p^k$$

gilt, mit ungerader Primzahl p und $k \in \mathbb{N}$.

Bemerkung 3.3.3. Ein *Körper* ist ein kommutativer Ring K, dessen Einheitengruppe mit der multiplikativen Gruppe $(K \setminus 0, \cdot)$ übereinstimmt. Insbesondere ist $1 \neq 0$, also K nicht der Nullring.

Für $a \in R$ definiert man die Potenzen a^n rekursiv durch $a^0 = 1$ und $a^{n+1} = a^n \cdot a$.

Definition 3.6. Ein Element a in R heißt *Linksnullteiler*, falls ein $x \neq 0$ in R existiert mit $ax = 0$. Es heißt *Rechtsnullteiler*, falls ein $y \neq 0$ in R existiert mit $ya = 0$. Ein Element, das sowohl ein Links- als auch Rechtsnullteiler ist, heißt *Nullteiler*. Ein Element $a \in R$ heißt *nilpotent*, wenn es ein $n \in \mathbb{N}$ gibt mit $a^n = 0$.

Beispiel 3.3.4. *Die Nullteiler des Ringes $\mathbb{Z}/12\mathbb{Z}$ sind gegeben durch die Nicht-Einheiten*

$$[0], [2], [3], [4], [6], [8], [9], [10],$$

und die nilpotenten Elemente sind gegeben durch $[0]$ *und* $[6]$.

Lemma 3.3.5. *Sei R ein Ring und $a \in R$ nilpotent. Dann sind $1-a$ und $1+a$ Einheiten von R.*

Beweis. Sei $a^n = 0$ mit $n \in \mathbb{N}$. Dann gilt

$$\begin{aligned} 1 &= 1 - a^n \\ &= (1-a)(1 + a + a^2 + \cdots + a^{n-1}) \\ &= (1 + a + a^2 + \cdots + a^{n-1})(1-a), \end{aligned}$$

und $1-a$ ist eine Einheit. Ersetzt man a durch $-a$, so folgt auch, dass $1+a$ eine Einheit ist. □

Allgemeine Ringe sind für viele unserer Fragestellungen zu kompliziert und ungeeignet. Deshalb wollen wir ab jetzt annehmen, dass alle Ringe *kommutativ* sind. Wir nennen einen Ring *nullteilerfrei*, wenn nur Null ein Nullteiler ist, d.h., aus $xy = 0$ folgt, dass entweder $x = 0$ oder $y = 0$ gilt.

Definition 3.7. Sei R (immer kommutativ) ein Ring mit $1 \neq 0$. R heißt *Integritätsring*, wenn er nullteilerfrei ist.

Beispiel 3.3.6. *Jeder Körper ist ein Integritätsring, und jeder Unterring eines Integritätsringes ist ein Integritätsring. Insbesondere sind $\mathbb{Z}, \mathbb{Z}[i]$ und $\mathbb{Z}/p\mathbb{Z}$, p prim, Integritätsringe.*

Beispiel 3.3.7. *Der Produktring $R \times S$ zweier Integritätsringe ist kein Integritätsring.*

Es gilt nämlich $(1,0) \cdot (0,1) = (0,0)$, mit $(1,0), (0,1) \in R \setminus 0$. Allgemeiner ist $R \times S$, R und S verschieden vom Nullring, kein Integritätsring.

In R schreiben wir $n \cdot x$ für $(1_R + \cdots + 1_R) \cdot x$ mit n Summanden. Die Abbildung $\chi \colon \mathbb{Z} \to R$ mit $n \mapsto n \cdot 1_R$ ist ein Ringhomomorphismus. Sein Kern ist ein Ideal in $\mathbb{Z}$, also von der Form $m\mathbb{Z}$ für eine eindeutig bestimmte natürliche Zahl m.

Definition 3.8. Die *Charakteristik* eines Ringes R ist die eindeutig bestimmte natürliche Zahl m mit $\ker(\chi) = m\mathbb{Z}$. Ist χ injektiv, so gilt $m = 0$. Ansonsten ist m die kleinste positive Zahl für die $n \cdot 1_R = 0$ gilt. Sie wird mit $char(R)$ bezeichnet.

Beispiel 3.3.8. *Es gilt* $char(\mathbb{Z}) = 0$, $char(\mathbb{Q}) = 0$ *und* $char(\mathbb{Z}/n\mathbb{Z}) = n$ *für alle* $n > 0$.

Lemma 3.3.9. *Sei* R *ein Integritätsring mit* $char(R) \neq 0$. *Dann ist die Charakteristik von* R *eine Primzahl.*

Beweis. Ist $char(R) = n = ab$ mit $1 < a, b < n$, so hat man

$$0 = n \cdot 1_R = (a \cdot 1_R)(b \cdot 1_R)$$

Da R keine Nullteiler hat, ist entweder $a \cdot 1_R = 0$ oder $b \cdot 1_R = 0$. Das steht aber im Widerspruch zur Minimalität von n in 3.8. Also ist n nicht zusammengesetzt. □

3.4 Hauptidealringe und Euklidische Ringe

Für $a \in R$ ist die Menge $(a) = \{xa \mid a \in R\}$ ein Ideal. Solche Ideale werden *Hauptideale* genannt. Man schreibt auch $Ra = aR = (a)$. Ist a eine Einheit, so ist $(a) = (1) = R$, denn $a \in (1) = R$ und $1 \in (a)$ wegen $1 = a \cdot a^{-1} \in (a)$. Für jede Teilmenge $M \subseteq R$ ist

$$(M) = \left\{ \sum_{i=1}^{m} x_i a_i \mid m \in \mathbb{N}, x_i \in R, a_i \in M \right\}$$

ein Ideal in R. Es ist das kleinste Ideal von R, das M enthält. Man erhält es als Schnitt über alle Ideale, die M enthalten. Man bezeichnet (M) als das von M *erzeugte* Ideal in R.

Definition 3.9. Ein Ideal I in R heißt *endlich erzeugt*, wenn es eine endliche Menge M in R gibt mit $(M) = I$. Ist $M = \{a_1, \ldots, a_n\}$, so schreibt man auch

$$I = (a_1, \ldots, a_n).$$

Definition 3.10. Ein Integritätsring R, in dem jedes Ideal ein Hauptideal ist, heißt *Hauptidealring*, oder einfach nur *HIR*.

Beispiel 3.4.1. 1. *Nach Satz* 3.2.5 *ist* $\mathbb{Z}$ *ein Hauptidealring. Jedes Ideal* I *hat die Form* $(n) = n\mathbb{Z}$ *für ein* $n \in \mathbb{N}$.

2. $\mathbb{Z}/4\mathbb{Z}$ *ist kein Hauptidealring, obwohl alle Ideale Hauptideale sind.*

Allerdings ist $\mathbb{Z}/4\mathbb{Z}$ kein Integritätsring wegen $[2] \cdot [2] = [0]$.

Viele Hauptidealringe besitzen noch eine stärkere Eigenschaft, nämlich dass sie Euklidisch sind.

Definition 3.11. Ein Integritätsring R heißt *Euklidisch*, falls es eine Abbildung $d\colon R \setminus 0 \to \mathbb{N}$ gibt, so dass zu je zwei Elementen $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ existieren mit

$$a = qb + r,$$

wobei entweder $r = 0$ oder $d(r) < d(b)$ ist. Die Abbildung d heißt dann *Gradabbildung*, oder *Euklidische Funktion*.

Zum Beispiel ist $\mathbb{Z}$ mit der Gradabbildung $f(n) = |n|$ Euklidisch. Der Name Gradabbildung kommt von dem Beispiel des Polynomringes $K[X]$, wo $d(f) = \deg(f)$ tatsächlich der Grad von f ist. Dieser Ring ist auch Euklidisch, wenn K ein Körper ist. Der folgende Satz ist sehr hilfreich für die Untersuchung von Hauptidealringen.

Satz 3.4.2. *Jeder Euklidische Ring R ist ein Hauptidealring.*

Beweis. Zu gegebenem Ideal $I \neq 0$ besitzt die Menge $\{d(b) \mid b \in I \setminus 0\}$ nicht-negativer ganzer Zahlen ein kleinstes Element, d.h., es existiert ein $c \neq 0$ in I mit $d(c) \leq d(b)$ für alle $b \neq 0$ in I. Nach Annahme existieren nun für jedes $b \in I$ $q, r \in R$ mit $b = qc + r$ mit $r = 0$ oder $d(r) < d(c)$. Da c minimal war, folgt $r = 0$ und $b = qc \in (c)$. Also ist $(c) \subseteq I \subseteq (c)$, d.h. $I = (c)$ ist ein Hauptideal. □

Beispiel 3.4.3. *Der Ring $\mathbb{Z}[i]$ ist Euklidisch, und daher ein Hauptidealring.*

Tatsächlich ist es leichter zu zeigen, dass $\mathbb{Z}[i]$ mit $d(a + bi) = a^2 + b^2$ Euklidisch ist, als die Definition von Hauptidealring zu verwenden.

Bemerkung 3.4.4. Die Umkehrung des obigen Satzes gilt nicht. Es gibt Hauptidealringe, die nicht Euklidisch sind. Das bekannteste Beispiel dürfte der Ring

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$$

sein. Zum Beweis siehe Frage 998716 in StackExchange Mathematics, und deren Links. Ein etwas unbekannteres Beispiel ist der Faktorring

$$\mathbb{R}[x, y]/(x^2 + y^2 + 1).$$

Sei $d \in \mathbb{Z}$ quadratfrei. Die Menge

$$\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\} \subseteq \mathbb{C}$$

ist ein Unterkörper von $\mathbb{C}$. Sei $z = a + b\sqrt{d}$ ein Element, dann definiert man die *Norm* von z durch

$$N(z) = z\overline{z} = x^2 - dy^2,$$

wobei $\overline{z} = x - y\sqrt{d}$ das zu z konjugierte Element genannt wird, auch wenn z reell ist. Man kann nachrechnen, dass $N(wz) = N(w)N(z)$ gilt für alle $z, w \in \mathbb{Q}(\sqrt{d})$. Dann definiert man

$$\mathcal{O}_d = \{a + b\omega_d \mid a, b \in \mathbb{Z}\},$$

wobei

$$\omega_d = \begin{cases} \sqrt{d}, & \text{if } d \equiv 2, 3(4), \\ \frac{1}{2}(1 + \sqrt{d}), & \text{if } d \equiv 1(4). \end{cases}$$

Als Unterring von $\mathbb{C}$ ist $\mathcal{O}_d$ ein Integritätsring, den man den *Ring der ganzen Zahlen* in $\mathbb{Q}(\sqrt{d})$ nennt. Für $d = 1$ erhält man $\mathcal{O}_1 = \mathbb{Z}$ in $\mathbb{Q}$, und für $d = -1$ hat man $\mathcal{O}_{-1} = \mathbb{Z}[i]$ in $\mathbb{Q}(i)$. Wir nennen einen Ring $\mathcal{O}_K$ der ganzen Zahlen eines Zahlkörpers K, der ein endlicher-dimensionaler Vektorraum über $\mathbb{Q}$ ist, *Norm-Euklidisch*, falls er Euklidisch ist mit der Norm $N(z) = z\overline{z}$ ist. Für $K = \mathbb{Q}(\sqrt{d})$ mit $d \neq 1$ und d quadratfrei gilt $\dim_{\mathbb{Q}}(K) = 2$, weswegen man K einen *quadratischen* Zahlkörper nennt.

Theorem 3.4.5. *Die Ringe $\mathcal{O}_d$ für quadratfreies $d < 0$ sind genau dann Euklidisch, wenn*

$$d = -1, -2, -3, -7, -11$$

gilt, und in diesen Fällen ist $\mathcal{O}_d$ Norm-Euklidisch.

Für quadratfreies $d > 0$ kennt man nur die Klassifikation der Norm-Euklidischen Ringe.

Theorem 3.4.6. *Die Ringe $\mathcal{O}_d$ für quadratfreies $d > 0$ sind genau dann Norm-Euklidisch, wenn*

$$d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$$

gilt.

Bemerkung 3.4.7. M. Harper [2] zeigte, dass der Ring $\mathcal{O}_{14}$ Euklidisch ist, obwohl er nicht Norm-Euklidisch ist. Allerdings kennt bisher niemand die Gradabbildung dazu explizit.

Auch die Frage, welche $\mathcal{O}_d$ Hauptidealringe sind, ist nur für $d < 0$ bekannt, siehe [7].

Theorem 3.4.8 (Baker-Heegner-Stark)**.** *Die Ringe $\mathcal{O}_d$ für quadratfreies $d < 0$ sind genau dann Hauptidealringe, wenn*

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

gilt.

Für $d > 0$ hat Gauß vermutet, dass $\mathcal{O}_d$ ein Hauptidealring für unendliche viele (quadratfreie) d ist. Die bekannte Liste dieser Zahlen beginnt mit $d = 1, 2, 3, 5, 6, 7, 11, 13, 14$.

3.5 Polynomringe

Wir erinnern nochmal daran, dass alle Ringe kommutativ sind.

Definition 3.12. Sei R ein Ring. Der *Polynomring* $R[X]$ in einer Unbestimmten X ist die Menge aller formalen Summen

$$\sum_{i=0}^{n} a_i X^i$$

mit $n \in \mathbb{N}_0$ und $a_i \in R$, zusammen mit folgender Addition und Multiplikation

$$\sum_{i=0}^{n} a_i X^i + \sum_{i=0}^{m} b_i X^i = \sum_{i=0}^{\max(n,m)} (a_i + b_i) X^i,$$

$$\left(\sum_{i=0}^{n} a_i X^i\right)\left(\sum_{i=0}^{m} b_i X^i\right) = \sum_{i=0}^{n+m} \left(\sum_{p+q=i} a_p b_q\right) X^i$$

Hier setzen wir $a_i = 0$ für $i \geq n+1$ und $b_i = 0$ für $i \geq m+1$.

Das Nullelement von $R[X]$ ist das Nullpolynom $0 = 0X^0$, und das Einselement ist $1 = 1X^0$. Die Abbildung

$$R \hookrightarrow R[X], \quad a \mapsto aX^0$$

ist ein injektiver Ringhomomorphismus. Er gestattet es, R als Unterring von $R[X]$ aufzufassen.

Definition 3.13. Sei $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ ein Polynom. Der *Grad* von f ist die größte natürliche Zahl $n \in \mathbb{N}_0$ mit $a_n \neq 0$, oder $-\infty$, falls alle $a_i = 0$ sind, d.h., $\deg(0) = -\infty$. Man schreibt $\deg(f) = n$ und a_n heißt der *Leitkoeffizient* von f. Ein Polynom $f \neq 0$ heißt *normiert*, falls $a_n = 1$ gilt mit $n = \deg(f)$.

Das einzige normierte Polynom vom Grad 0 ist $1X^0 = 1 = 1_R$. Nur das Nullpolynom hat Grad $-\infty$.

Lemma 3.5.1. *Es seien $f, g \in R[X]$ Polynome über R. Dann gilt*

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\},$$
$$\deg(fg) \leq \deg(f) + \deg(g)$$

Sind die Leitkoeffizienten von f und g keine Nullteiler, also zum Beispiel wenn R ein Integritätsring ist, so gilt die Gleichheit

$$\deg(fg) = \deg(f) + \deg(g).$$

Beweis. Ist entweder $f = 0$ oder $g = 0$, so gilt die Behauptung, wenn man die Konventionen $(-\infty)+(-\infty) = -\infty$ und $(-\infty)+n = -\infty$ beachtet. Andernfalls gilt $\deg(f) = n$, $\deg(g) = m$ mit $n, m \in \mathbb{N}_0$. Ist $f = \sum_{i=0}^{n} a_i X^i$ und $g = \sum_{i=0}^{m} b_i X^i$, so ist $a_i + b_i = 0$ für $i > \max(n, m)$. Also ist der Grad von $f + g$ höchstens so gross wie $\max(n, m)$. Für die zweite Ungleichung beachte man, dass $\sum_{p+q=i} a_p b_q = 0$ ist für $i \geq n+m$. Der Koeffizient vom Grad $n+m$ in fg ist $a_n b_m$. Ist R ein Integritätsring, oder sind a_n, b_m keine Nullteiler in R, so folgt aus $a_n, b_m \neq 0$ auch $a_n b_m \neq 0$. Dann gilt

$$\deg(fg) = n + m = \deg(f) + \deg(g).$$

□

Korollar 3.5.2. *Der Polynomring $R[X]$ ist genau dann ein Integritätsring, wenn R ein Integritätsring ist. Dann hat man $R[X]^\times = R^\times$.*

Beweis. Ist $R[X]$ nullteilerfrei, so auch sein Unterring R. Sei R nullteilerfrei und $f \in R[X]$ ein Nullteiler von $R[X]$ mit $fg = 0$ für ein $g \neq 0$. Dann folgt wegen Lemma 3.5.1

$$-\infty = \deg(0) = \deg(fg) = \deg(f) + \deg(g),$$

also $\deg(f) = -\infty$ und $f = 0$. Somit ist auch $R[X]$ nullteilerfrei.
Sei nun $f \in R[X]^\times$. Dann gibt es ein $g \in R[X]$ mit $fg = 1$. Lemma 3.5.1 ergibt

$$0 = \deg(fg) = \deg(f) + \deg(g),$$

also $\deg(f) = \deg(g) = 0$ und damit $f, g \in R^\times$. Somit ist

$$R[X]^\times \subseteq R^\times \subseteq R[X]^\times.$$

□

Satz 3.5.3. *Sei $g \neq 0$ ein Polynom in $R[X]$, dessen Leitkoeffizient eine Einheit in R ist. Dann existieren zu jedem Polynom $f \in R[X]$ eindeutig bestimmte Polynome $q, r \in R[X]$, so dass $f = qg + r$ mit $\deg(r) < \deg(g)$ gilt.*

Beweis. Die Fälle $f = 0$ bzw. $f \neq 0, \deg(f) < \deg(g)$ sind klar mit $q = 0$ und $r = f$. Sei also $m = \deg(f) \geq \deg(g) = n$. Wir führen eine Induktion über m. Sei $f = \sum_{i=0}^{m} a_i X^i$ und $g = \sum_{i=0}^{n} b_i X^i$ mit $b_n \in R^\times$. Der Grad des Polynoms

$$h = f - a_m b_n^{-1} X^{m-n} g$$

ist echt kleiner als m, weil sich das Leitmonom $a_m X^m$ von f mit dem von $a_m b_n^{-1} X^{m-n} g$ weghebt. Also gibt es nach Induktionsvoraussetzung $q_0, r \in R[X]$ mit $\deg(r) < n$, so dass $h = q_0 g + r$ ist. Daraus folgt

$$\begin{aligned} f &= (a_m b_n^{-1} X^{m-n} + q_0)g + r \\ &= qg + r. \end{aligned}$$

Nun fehlt nur noch die Eindeutigkeit von q und r zu zeigen. Angenommen, $f = q_1 g + r_1 = q_2 g + r_2$ mit $\deg(r_1), \deg(r_2) < \deg(g)$. Dann ist

$$(q_2 - q_1)g = r_2 - r_1.$$

Da b_n eine Einheit in R ist, gilt nach Lemma 3.5.1

$$\begin{aligned} \deg(g) > \deg(r_2 - r_1) &= \deg((q_2 - q_1)g \\ &= \deg(q_2 - q_1) + \deg(g). \end{aligned}$$

Das kann nur stimmen, wenn $q_2 - q_1$ das Nullpolynom vom Grad $-\infty$ ist, also für $q_2 = q_1$, und dann $r_2 = r_1$. □

Korollar 3.5.4. *Sei K ein Körper. Dann ist $K[X]$ mit der Gradfunktion $d(f) = \deg(f)$ ein Euklidischer Ring.*

3.6 Primideale und maximale Ideale

Definition 3.14. Sei R ein Ring.

(1) Ein Ideal $P \subset R$ heißt *prim* oder *Primideal*, wenn $P \neq R$ und wenn für alle $a, b \in R$ aus $ab \in P$ auch $a \in P$ oder $b \in P$ folgt.

(2) Ein Ideal $M \subset R$ heißt *maximal* oder *maximales Ideal*, wenn $M \neq R$ und wenn es kein Ideal I gibt mit $M \subsetneq I \subsetneq R$, d.h. wenn für alle Ideale $I \subseteq R$ mit $M \subseteq I$ gilt $I = M$ oder $I = R$.

Das Ideal $I = 0$ ist nach Definition genau dann ein Primideal, wenn I ein Integritätsring ist. In $\mathbb{Z}$ ist jedes Ideal von der Form $n\mathbb{Z}$ mit $n \in \mathbb{N}$.

Beispiel 3.6.1. *Sei $m \in \mathbb{N}$. Ein Ideal $m\mathbb{Z}$ in $\mathbb{Z}$ ist genau dann prim, wenn $m = 0$ oder m prim ist. Es ist genau dann maximal, wenn m prim ist.*

Das folgt direkt aus den Definitionen. Allerdings kann man auch den folgenden Satz anwenden.

Satz 3.6.2. *Sei R ein Ring.*

(1) *Ein Ideal $P \subset R$ ist genau dann prim, wenn R/P ein Integritätsbereich ist.*

(2) *Ein Ideal $M \subset R$ ist genau dann maximal, wenn R/M ein Körper ist.*

Beweis. Zu (1): Ist $P \subset R$ ein Primideal, so ist $P \neq R$ und somit $R/P \neq 0$. Gilt $[a][b] = 0$ für $a, b \in R/P$, so ist $ab \in P$, also entweder $a \in P$ oder $b \in P$. Das bedeutet, entweder $[a] = 0$ oder $[b] = 0$. Somit ist R/P nullteilerfrei. Sei umgekehrt R/P ein Integritätsbereich. Da $R/P \neq 0$ ist, gilt $R \neq P$. Ist $ab \in P$, so folgt $[a][b] = 0$. Da R/P nullteilerfrei ist, folgt $[a] = 0$ oder $[b] = 0$. Das bedeutet, $a \in P$ oder $b \in P$.

Zu (2): Für jedes Ideal $I \supseteq M$ ist das Bild $\pi(I)$ unter der Restklassenabbildung $\pi\colon R \to R/M$ ein Ideal in R/M. Umgekehrt ist für jedes Ideal $J \subseteq R/M$ das Urbild $\pi^{-1}(J)$ ein Ideal in R, das M enthält. Dann sind

$$\begin{aligned} \{\text{Ideale } I \subseteq R \text{ mit } M \subseteq I\} &\longleftrightarrow \{\text{Ideale } J \subseteq R/M\} \\ I &\mapsto \pi(I) \\ \pi^{-1}(J) &\mapsfrom J \end{aligned}$$

zueinander inverse Bijektionen. Ist R/M ein Körper, so hat R/M nur die zwei Ideale 0 und R/M. In der Tat, jeder Körper K hat nur die beiden Ideale 0 und K, weil jedes Ideal $I \neq 0$ ein $a \neq 0$ enthält, also auch $1 = aa^{-1}$ enthält, und somit $I = (1) = R$ gilt. Mit den obigen Bijektionen folgt daraus, dass M ein maximales Ideal in R ist.

Ist umgekehrt M ein maximales Ideal von R, so ist R/M nicht der Nullring. Mit der obigen Bijektion folgt, dass R/M nur die Ideale 0 und R/M besitzt. Jeder Ring S, der nicht der Nullring ist und nur die Ideale 0 und S besitzt ist ein Körper, weil jedes $s \neq 0$ in S invertierbar ist. Denn (s) ist ein Ideal ungleich Null, also $(s) = S$, und somit $sx = 1$ für ein $x \in S$. Also ist R/M ein Körper. □

Beispiel 3.6.3. *Der Ring $\mathbb{Z}/mZ$ ist genau dann ein Körper, wenn m eine Primzahl ist. Wir schreiben dann $m = p$ und $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.*

Ist $m = p$ prim, so ist $p\mathbb{Z}$ ein maximales Ideal in $\mathbb{Z}$. Also ist $Z/p\mathbb{Z}$ ein Körper. Ist m nicht prim, so ist $\mathbb{Z}/m\mathbb{Z}$ nicht nullteilerfrei, und daher kein Körper.

Korollar 3.6.4. *Jedes maximale Ideal in R ist ein Primideal.*

Beweis. Ist M ein maximales Ideal in R, so ist R/M ein Körper, also insbesondere ein Integritätsring. Somit ist M prim. □

Tatsächlich ist es nicht so klar, dass ein Ring R (immer kommutativ) überhaupt ein maximales Ideal besitzt. Um das zu zeigen, braucht man das Zornsche Lemma.

Satz 3.6.5. *Jeder Ring $R \neq 0$ besitzt ein maximales Ideal.*

Beweis. Die Menge $\mathcal{M}$ aller Ideale $I \neq (1)$ in R ist nicht leer, da $(0) \in \mathcal{M}$. Sie ist durch die Inklusionsrelation geordnet. Um Zorns Lemma anzuwenden, müssen wir zeigen, dass jede Kette in $\mathcal{M}$ eine obere Schranke in $\mathcal{M}$ hat. Sei T also eine Kette von Idealen $I \neq (1)$. Dann betrachte man

$$J := \bigcup_{I \in T} I.$$

Dann ist J ein Ideal in R, denn für alle $x, y \in J$ existiert ein $I \in T$ mit $x, y \in I$. Da I ein Ideal ist, folgt $x - y \in I$ und $rx \in I$ für alle $r \in R$. Weiterhin gilt $1 \notin J$, da $1 \notin I$ für alle $I \in T$. Also gilt $J \in \mathcal{M}$, und J ist offensichtlich eine obere Schranke der Kette T. Aus Zorns Lemma folgt die Existenz eines maximalen Elementes für $\mathcal{M}$. □

Korollar 3.6.6. *Sei I ein echtes Ideal in R. Dann gibt es ein maximales Ideal M in R mit $I \subseteq M$.*

Beweis. Man betrachte im obigen Satz den Ring R/I und verwende die Bijektion aus dem Beweis von (2) in Satz 3.6.2. □

3.7 Bruchringe und Quotientenkörper

In der kommutativen Algebra werden sogenannte *Lokalisierungen* eines Ringes R bezüglich einer multiplikativ abgeschlossenen Teilmenge S studiert. Man erhält einen neuen Ring $S^{-1}R$, in dem die Elemente von S invertierbar sind. Er heißt auch *Ring der Brüche*. Ist R ein Integritätsring, so erhält man mit $S = R \setminus 0$ den sogenannten *Quotientenkörper* von R. Für $R = \mathbb{Z}$ ist das genau die Konstruktion, aus der man $\mathbb{Q}$ erhält.

Definition 3.15. Eine Teilmenge S von R heißt *multiplikativ abgeschlossen*, wenn gilt

(1) $1 \in S$,

(2) Aus $a \in S$, $b \in S$ folgt $ab \in S$.

Beispiel 3.7.1. 1. *Sei I ein Ideal in R. Dann ist $R \setminus I$ genau dann multiplikativ abgeschlossen, wenn I ein Primideal ist.*

2. *Ist R ein Integritätsring, so ist $R \setminus 0$ multiplikativ abgeschlossen.*

3. *Die Menge aller Nicht-Nullteiler in R ist multiplikativ abgeschlossen.*

4. *Die Menge aller Einheiten in R ist multiplikativ abgeschlossen.*

Sei S eine multiplikative abgeschlossenen Teilmenge von R. Wir definieren eine Relation auf der Menge aller geordneten Paare von $R \times S$ wie folgt. Für zwei Paare $(a,s),(b,t) \in R \times S$ sei

$$(a,s) \sim (b,t) \Longleftrightarrow (at-bs)u = 0 \text{ für irgendein } u \in S.$$

Lemma 3.7.2. *Die Relation $\sim$ definiert eine Äquivalenzrelation auf $R \times S$.*

Beweis. Es ist klar, dass $(a,s) \sim (a,s)$ gilt, und $(a,s) \sim (b,t)$ auch $(b,t) \sim (a,s)$ impliziert. Es ist also nur die Transitivität zu zeigen. Es gelte also $(a,s) \sim (b,t)$ und $(b,t) \sim (c,r)$. Es existieren also $v,w \in S$ mit

$$(at-bs)v = 0, \quad (br-ct)w = 0.$$

Daraus folgt

$$(at-bs)rvw = 0, \quad (br-ct)svw = 0,$$

und damit $atrvw = bsrvw = ctsvw$, so dass

$$(ar-cs)tvw = 0.$$

Da S multiplikativ abgeschlossen ist, haben wir $tvw \in S$, also $(a,s) \sim (c,r)$. □

Wir schreiben einfach $\frac{a}{s}$ für die Äquivalenzklasse von (a,s).

Definition 3.16. Der *Ring der Brüche* bezüglich S ist der Ring

$$S^{-1}R := \{a/s \mid (a,s) \in R \times S\},$$

wobei die Addition und die Multiplikation auf $S^{-1}R$ durch

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st},$$
$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

gegeben sind.

Bemerkung 3.7.3. Addition und Multiplikation sind wohldefiniert, d.h. hängen nicht von der Wahl der Vertreter (a,s) und (b,t) ab. Das Nachrechnen der Ringaxiome ist Routine. Der Ring $S^{-1}R$ hat das Nullelement $\frac{0}{1}$ und das Einselement $\frac{1}{1}$. Die Abbildung $\varphi\colon R \to S^{-1}R$ mit $r \mapsto \frac{r}{1}$ ist ein Ringhomomorphismus mit Kern

$$\ker(\varphi) = \{r \in R \mid \text{ es existiert ein } s \in S \text{ mit } rs = 0\ \}.$$

Es gilt genau dann $S^{-1}R = 0$ wenn $0 \in S$.

Definition 3.17. Sei R ein Integritätsring. Dann ist $S = R \setminus 0$ multiplikativ abgeschlossen und $S^{-1}R$ ein Körper. Er heißt der *Quotientenkörper* von R und wird mit $Quot(R)$ bezeichnet.

Die Abbildung $\varphi\colon R \to S^{-1}R$ ist dann injektiv, da S keine Nullteiler enthält. Also kann man R mit seinem Bild in $S^{-1}R$ identifizieren. Wie schon erwähnt ist $Quot(\mathbb{Z}) = \mathbb{Q}$. Ein anderes Beispiel ist $Quot(\mathbb{Z}[i]) = \mathbb{Q}(i)$.

3.8 Teilbarkeit und faktorielle Ringe

In der elementaren Zahlentheorie wurde die eindeutige Primfaktorzerlegung von ganzen Zahlen studiert. Solche Zerlegungen sind nicht nur für den Ring $\mathbb{Z}$ interessant, sondern auch allgemein für Integritätsringe. Allerdings haben Primfaktorzerlegungen dort nicht immer so schöne Eigenschaften wie in $\mathbb{Z}$.

Definition 3.18. Sei R ein Integritätsring.

(1) Für Elemente $a, b \in R$ sagt man a *teilt* b, oder $a \mid b$, falls es ein $c \in R$ gibt mit $ac = b$.

(2) Zwei Elemente $a, b \in R$ heißen *assoziiert*, oder $a \sim b$, falls $a \mid b$ und $b \mid a$ gilt.

(3) Ein Element $p \in R$ heißt *prim* oder *Primelement*, falls $p \neq 0$ und p keine Einheit ist, und für alle $a, b \in R$ mit $p \mid ab$ folgt $p \mid a$ oder $p \mid b$.

(4) Ein Element $u \in R$ heißt *irreduzibel*, falls $u \neq 0$ und u keine Einheit ist, und aus einer Darstellung $u = ab$ mit $a, b \in R$ immer folgt, dass a oder b eine Einheit ist.

Beispiel 3.8.1. *Für $R = \mathbb{Z}$ sind die Primelemente genau alle Zahlen $\{\pm p\}$, wobei p eine Primzahl ist. Ebenso sind auch alle irreduziblen Elemente gegeben. Die Begriffe prim und irreduzibel sind also äquivalent in $\mathbb{Z}$.*

Zwei ganze Zahlen m und n sind genau dann assoziiert, wenn $m = \pm n$ gilt, d.h., wenn sie sich durch eine Einheit in $\mathbb{Z}$ unterscheiden. Sind allgemein $a, b \in R$ assoziiert, so gilt $a = \mu b$ und $b = \nu a$ für $\mu, \nu \in R$, also $b = \nu\mu b$, und somit $b(1 - \nu\mu) = 1$. Ist $b \neq 0$, so sind μ, ν Einheiten. Für $b = 0$ ist $a = 0$ und $b = 1 \cdot a$. Also gilt

$$a \sim b \Longleftrightarrow a = \mu b \text{ mit einer Einheit } \mu.$$

Ein Körper hat gar keine Primelemente, da alle Elemente ungleich Null Einheiten sind. Ebenso hat er auch keine irreduziblen Elemente.

Wir können obige Begriffe auch idealtheoretisch beschreiben.

Lemma 3.8.2. *Sei R ein Integritätsring.*

(1) Es gilt $(a) \supseteq (b) \Longleftrightarrow a \mid b$. "To contain is to divide".

(2) Es gilt $a \sim b \Longleftrightarrow (a) = (b)$.

(3) Ein Element $p \in R$ ist genau dann prim, wenn $p \neq 0$ und (p) ein Primideal in R ist.

(4) Ist R ein Hauptidealring, dann ist ein Element $u \in R$ genau dann irreduzibel, wenn (u) ein maximales Ideal in R ist.

Beweis. Wir überlassen $(1) - (3)$ dem Leser. (4) folgt aus (1), weil in einem Hauptidealring jedes Ideal von der Form (a) ist. Also ist (a) genau dann maximal wenn a keine nicht-trivialen Teiler hat, genau dann wenn a irreduzibel ist. □

Das folgende Beispiel zeigt, dass (4) nicht in jedem Integritätsring gelten muss.

Beispiel 3.8.3. *Das Polynom X in $R = \mathbb{Z}[X]$ ist ein irreduzibles Element, aber das Ideal (X) ist nicht maximal.*

In der Tat, da $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$ kein Körper ist, kann (X) kein maximales Ideal sein. Die Aussage in (4) kann verbessert werden, idem man sagt, dass ein Element $r \in R$ genau dann irreduzibel ist, wenn das Ideal (a) maximal unter den Hauptidealen in R ist. Für Hauptidealringe sind die Begriffe prim und irreduzibel sogar äquivalent.

Satz 3.8.4. *Sei R ein Integritätsring.*

(1) Jedes Primelement in R ist irreduzibel.

(2) In einem Hauptidealring R ist ein Element genau dann prim wenn es irreduzibel ist.

(3) In einem Hauptidealring R ist ein Ideal ungleich Null genau dann prim wenn es maximal ist.

Beweis. Zu (1). Sei p ein Primelement in R und $p = ab$. Dann gilt $a \mid p$ und $b \mid p$. Da p prim ist, folgt auch $p \mid a$ oder $p \mid b$. Im ersten Fall ist $p \sim a$ und deshalb $b \in R^\times$, und im zweiten Fall $p \sim b$, also $a \in R^\times$. Also ist p irreduzibel.

Zu (2). Sei $u \in R$ irreduzibel. Wegen Lemma 3.8.2, (4) für Hauptidealringe ist (u) ein maximales Ideal, also auch ein Primideal. Somit ist u ein Primelement. Die Umkehrung gilt allgemein wegen (1).

Zu (3). Das folgt aus Lemma 3.8.2, (3) und (4). □

Satz 3.8.5. *Der Polynomring $R[X]$ ist genau dann ein Hauptidealring, wenn R ein Körper ist.*

Beweis. Die Abbildung $R[X] \to R$, $f \mapsto f(0)$ ist ein Ringepimorphismus mit Kern (X). Nach dem Isomorphiesatz gilt also $R[X]/(X) \cong R$. Sei $R[X]$ ein Hauptidealring. Dann ist das Ideal $I = (X)$ prim, da $R[X]/(X) \cong R$ als Unterring von $R[X]$ selbst ein Integritätsring ist. Wegen 3.8.4, (2) ist (X) auch maximal, und somit $R/I \cong R$ ein Körper. Umgekehrt sei R ein Körper. Dann ist $R[X]$ ein Euklidischer Ring mit der Gradfunktion $d(f) = \deg(f)$, also auch ein Hauptidealring, siehe Satz 3.4.2. □

Definition 3.19. Sei R ein Integritätsring und $a, b \in R$.

(1) Ein *größter gemeinsamer Teiler*, oder ein *ggT* von a und b ist ein $d \in R$ mit $d \mid a$, $d \mid b$ und der Eigenschaft, dass für alle $r \in R$ mit $r \mid a$, $r \mid b$ folgt $r \mid d$. Wir schreiben $d = \gcd(a, b)$.

(2) Ein *kleinstes gemeinsames Vielfaches*, oder ein *kgV* von a und b ist ein $v \in R$ mit $a \mid v$, $b \mid v$, und der Eigenschaft, dass für alle $s \in R$ mit $a \mid s$, $b \mid s$ folgt $v \mid s$. Wir schreiben $v = \mathrm{l}cm(a, b)$.

Satz 3.8.6. *Sei R ein Integritätsring und $a, b \in R$.*

(1) Falls es in R einen ggT von a und b gibt, so ist er bis auf eine Einheit eindeutig.

(2) Falls es ein $d \in R$ gibt mit $(d) = (a, b)$, so ist d ein ggT von a und b.

(3) Falls es in R ein kgV von a und b gibt, so ist es bis auf eine Einheit eindeutig.

(4) Falls es ein $v \in R$ gibt mit $(v) = (a) \cap (b)$, so ist v ein kgV von a und b.

Beweis. Zu (1). Sind d und e zwei ggTs, so gilt $d \mid e$ und $e \mid d$. Damit gilt $d \sim e$, also $d = \mu e$ für eine Einheit μ.

Zu (2). Aus $(d) = (a, b)$ folgt $(a) \subseteq (d)$, $(b) \subseteq (d)$, also $d \mid a$, $d \mid b$. Wegen $d \in (a, b)$ gibt es $x, y \in R$ mit $d = xa + yb$. Gilt also $r \mid a$, $r \mid b$, so folgt $r \mid d$. Also ist d ein ggT von a und b.

Ähnlich zeigt man (3) und (4). □

Falls ein ggT oder kgV existiert, ist er also im wesentlichen eindeutig. Für Hauptidealringe haben wir folgdenes Resultat.

Satz 3.8.7. *Sei R ein Hauptidealring und $a, b \in R$. Dann gibt es einen ggT $d = \gcd(a, b)$ und es gilt $(d) = (a, b) = (a) + (b)$. Ebenso gibt es ein kgV $v = \mathrm{lcm}(a, b)$ und es gilt $(v) = (a) \cap (b)$.*

Beweis. Da R ein Hauptidealring ist, gibt es zu dem Ideal (a, b) ein $d \in R$ mit $(d) = (a, b)$. Wegen 3.8.6, (2) ist d ein ggT von a und b. Nach Definition ist (a, b) das kleinste Ideal das a und b enthält. Also gilt in jedem Ring $(a, b) = (a) + (b)$.

Da auch das Ideal $(a) \cap (b)$ ein Hauptideal ist, gibt es ein $v \in R$ mit $(v) = (a) \cap (b)$. Wegen 3.8.6, (4) ist v ein kgV von a und b. □

Definition 3.20. Zwei Elemente $a, b \in R$ heißen *teilerfremd*, falls 1 ein ggT von a und b ist. Zwei Ideale I und J in einem Ring heißen *teilerfremd*, falls $I + J = R$ gilt.

Aus Satz 3.8.7 folgt

Satz 3.8.8. *Sei R ein Hauptidealring. Dann sind a und b aus R genau dann teilerfremd, wenn die Ideale (a) und (b) teilerfremd sind. In diesem Fall gibt es $r, s \in R$ mit $ra + sb = 1$.*

Definition 3.21. Ein *faktorieller Ring* ist ein Integritätsring R, in dem sich jedes Element $a \in R$ mit $a \neq 0$, $a \notin R^\times$ als ein endliches Produkt von Primelementen schreiben läßt.

Wir nennen diese Darstellung als Produkt von Primelementen eine *Primfaktorzerlegung*. Das leere Produkt ist dabei eingeschlossen, also ist ein Körper auch ein faktoreller Ring. Er hat keine Nicht-Einheiten ungleich Null.

Bemerkung 3.8.9. Man kann leicht zeigen, dass Primfaktorzerlegungen, wenn sie existieren, *eindeutig* in folgendem Sinne sind. Gilt

$$\prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j$$

mit Primelementen $p_i, q_j \in R$, so folgt $m = n$ und es gibt eine Permutation $\sigma \in S_n$ und Einheiten ε_i in R mit $p_j = \varepsilon_j \cdot q_{\sigma(j)}$ für alle $j = 1, \ldots, n$.

Satz 3.8.10. *Ein Integritätsring R is genau dann faktoriell, wenn sich jedes Element $r \neq 0, r \notin R^\times$ als ein endliches Produkt von irreduziblen Elementen schreiben läßt, und diese Zerlegung bis auf Reihenfolge und Einheiten eindeutig ist.*

Beweis. Sei R faktoriell und $r \neq 0$ keine Einheit. Dann existiert eine eindeutige Zerlegung in Primelemente, d.h., $r = p_1 \cdots p_n$. Jedes Primelement ist aber irreduzibel nach Satz 3.8.4. Also erhalten wir eine eindeutige Zerlegung in irreduzible Elemente. Hat jedes Element eine Zerlegung in irreduzible Elemente, dann ist jedes irreduzible Element u auch prim. Denn hat man $u \mid ab$, so gibt es ein $c \in R$ mit $uc = ab$. Nun ersetze man a, b, c durch eine Zerlegung in irreduzible Elemente, d.h.,

$$a = p_1 \cdots p_r,\ b = q_1 \cdots q_s,\ c = r_1 \cdots r_t.$$

Dann erhält man aber auf beiden Seiten von $uc = ab$ im wesentlichen die gleiche Zerlegung, wegen der Eindeutigkeit der Zerlegungen,

$$ur_1 \cdots r_t = p_1 \cdots p_r \cdot q_1 \cdots q_s.$$

Also ist $u = p_i$ für ein i, oder $u = q_j$ für ein j und es folgt entweder $u \mid a$ oder $u \mid b$. Somit ist u auch prim und R faktoriell. □

Korollar 3.8.11. *Sei R ein faktorieller Ring. Dann ist ein Element $a \in R$ genau dann prim wenn es irreduzibel ist.*

Beispiel 3.8.12. 1. *Jeder Körper ist ein faktorieller Ring.*

2. *$\mathbb{Z}$ ist ein faktorieller Ring.*

3. *$\mathcal{O}_{-5} = \mathbb{Z}[\sqrt{-5}]$ ist kein faktorieller Ring.*

Zu 3. Sei $R = \mathcal{O}_{-5}$. Die Normabbildung $N\colon \mathcal{O}_d \to \mathbb{Z}$ ist durch

$$N(z) = z\overline{z} = (a + b\sqrt{-5})(a - \sqrt{-5}) = a^2 + 5b^2$$

gegeben. Es ist leicht zu sehen, dass z eine Einheit ist, genau dann wenn $N(z) = 1$ gilt. Das bedeutet, $R^\times = \{\pm 1\}$. Das Element $z = 6$ hat folgende Zerlegungen in irreduzible Elemente,

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Nun ist 2 kein Primelement, denn $2 \mid 6$, aber 2 teilt keinen der beiden Faktoren $1 \pm \sqrt{-5}$. Dazu bemerkt man, dass aus $z \mid w$ in R folgt $N(z) \mid N(w)$ in $\mathbb{Z}$. Aber

$$N(2) = 4 \nmid 6 = N(1 \pm \sqrt{-5}).$$

Andererseits ist 2 aber irreduzibel. Angenommen $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$, und ein Faktor, sagen wir der erste, wäre keine Einheit, d.h., $a^2+5b^2 \neq 1$. Dann gilt $(a+b\sqrt{-5}) \mid 2$ in R, also $a^2 + 5b^2 \mid 4$ in $\mathbb{Z}$. Dann bleibt nur $4 = 2 \cdot 2$ und $a^2 + 5b^2 = 2$, was aber keine Lösung in $\mathbb{Z}$ hat, ein Widerspruch. Wegen Korollar 3.8.11 kann R also nicht faktoriell sein.

Lemma 3.8.13. *Sei R ein faktorieller Ring. Dann gibt es zu gegebenem $a \neq 0$ in R nur endlich viele verschiedene Hauptideale (b) mit $(b) \supseteq (a)$ in R.*

Beweis. Ist a eine Einheit, so ist $(a) = R$ und die Aussage klar. Andernfalls hat man eine Zerlegung $a = u_1 \cdots u_n$ in irreduzible Elemente. Für $(b) \supseteq (a)$ gilt $b \mid a$, also $a = bq$ mit einem $q \in R$. Wegen der Eindeutigkeit der Zerlegung muss es $1 \leq i_1 < \cdots < i_m \leq n$ geben mit $b \sim u_{i_1} \cdots u_{i_m}$. Das sind nur endlich viele Möglichkeiten für (b). □

Satz 3.8.14. *Ein Integritätsbereich R ist genau dann ein faktorieller Ring, wenn jedes irreduzible Element prim ist und jede aufsteigene Kette von Hauptidealen*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

stationär wird.

Beweis. Sei R ein faktorieller Ring. Dann ist nach Korollar 3.8.11 jedes irreduzible Element prim. Wegen Lemma 3.8.13 wird jede aufsteigende Kette von Hauptidealen stationär.

Sei umgekehrt R ein Integritätsring mit aufsteigender Kettenbedingung für Hauptideale. Betrachte die Menge H aller Hauptideale (a) in R mit $a \neq 0$, $a \notin R^\times$, so dass a kein Produkt von irreduziblen Elementen ist. Wir müssen zeigen, dass $H = \emptyset$ ist und nehmen das Gegenteil an. Dann enthält H ein maximales Element I, denn andernfalls hätte man zu jedem $J_1 \in H$ ein $J_2 \in H$ mit $J_1 \subsetneq J_2$, und so durch Fortsetzen des Verfahrens eine aufsteigende Kette von Hauptidealen, die nicht stationär wäre. Sei $I = (a)$ für ein $a \in R$. Dann ist $a \neq 0$, keine Einheit und muss reduzibel sein. Also gibt es Nicht-Einheiten $b, c \in R$ mit $a = bc$. Man erhält echte Inklusionen $(a) \subsetneq (b)$ und $(a) \subsetneq (c)$. Also gehören wegen der Maximalität von (a) die Ideale (b) und (c) nicht zu H. Also sind b und c das Produkt irreduzibler Elemente, und somit auch $a = bc$. Das ist ein Widerspruch zu $(a) \in H$. Also ist H leer. □

Die aufsteigende Kettenbedingung kann man überhaupt für *alle* Ideale in einem beliebigen Ring fordern. Dann erhält man eine weitere wichtige Klasse von Ringen.

Definition 3.22. Ein Ring R heißt *Noethersch*, wenn jede aufsteigende Kette von Idealen

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

stationär wird.

Satz 3.8.15. *Sei R ein Ring. Dann sind die folgenden Aussagen äquivalent.*

(1) R ist Noethersch.

(2) Jede nicht-leere Menge von Idealen in R hat ein maximales Element bezüglich Inklusion.

(3) Jedes Ideal in R ist endlich erzeugt.

Beweis. (1) $\Rightarrow$ (2): Ist M eine nicht-leere Menge von Idealen, die kein maximales Element hat, so gibt es zu jedem $I_1 \in M$ ein $I_2 \in M$ mit $I_1 \subsetneq I_2$. Somit erhält man eine aufsteigende Kette von Idealen, die nicht stationär wird, im Widerspruch zur Annahme. Also folgt (2).

(2) $\Rightarrow$ (3): Sei I ein Ideal in R und $\mathcal{M}$ die Menge aller Ideale in A, die endlich erzeugt sind und in I enthalten sind. Dann ist $\mathcal{M}$ nicht-leer. Sei M ein maximales Element in $\mathcal{M}$ und $a \in I$. Dann gilt $(a) + M \in \mathcal{M}$ und $M \subseteq (a) + M$. Wegen der Maximalität folgt $M = (a) + M$, also $a \in M$. Also ist $I \subseteq M \subseteq I$, d.h., $I = M$. Da M nach Definition von $\mathcal{M}$ endlich erzeugt ist, folgt (3).

(3) $\Rightarrow$ (1): Ist $I_1 \subseteq I_2 \subseteq I_2 \subseteq \cdots$ eine aufsteigende Kette von Idealen in R, so ist ihre Vereinigung I wieder ein Ideal. Es ist endlich-erzeugt nach Voraussetzung, d.h., $I = (a_1, \ldots, a_m)$. Zu jedem $1 \leq j \leq m$ existiert ein n_j mit $a_j \in I_{n_j}$. Ist n_0 die größte der Zahlen n_j, so gilt $I = I_{n_0}$, und die Kette wird stationär. Also folgt (1). □

Korollar 3.8.16. *Jeder Hauptidealring ist faktoriell und Noethersch. Wir haben die Implikationen*

$$\textit{Euklidisch} \implies \textit{Hauptidealring} \implies \textit{faktoriell}$$

Beweis. Sei R ein Hauptidealring. Nach Satz 3.8.4 ist jedes irreduzible Element prim. Offensichtlich ist jedes Ideal in R von einem Element erzeugt. Nach (3) des obigen Satzes 3.8.15 ist R also Noethersch. Somit ist R faktoriell nach Satz 3.8.14. Euklidische Ringe sind Hauptidealringe nach Satz 3.4.2, und deshalb faktoriell. □

Beispiel 3.8.17. *Alle Ringe $\mathcal{O}_d$ mit*

$$d = -163, -67, -43, -19, -11, -7, -3, -2, -1, 1, 2, 3, 5, 6, 7, 11, 13, 14, \ldots$$

sind faktoriell, siehe Theorem 3.4.8.

Bemerkung 3.8.18. Die Umkehrungen der Implikationen aus Korollar 3.8.16 gelten im allgemeinen nicht. Wir werden noch sehen, dass $\mathbb{Z}[X]$ ein faktorieller Ring ist. Er ist aber kein Hauptidealring, da $\mathbb{Z}$ kein Körper ist, siehe Satz 3.8.5. Allerdings, Ganzzahlringe in Zahlkörpern sind genau dann faktoriell, wenn sie Hauptidealringe sind. Das gilt insbesondere für die Ringe $\mathcal{O}_d$.

3.9 Der Satz von Gauß

Der Satz von Gauß besagt, dass der Poylnomring $R[X]$ über einem faktoriellen Ring R wieder faktoriell ist. Für $R = \mathbb{Z}$ erhält man also, dass der Ring $\mathbb{Z}[X]$ faktoriell ist. Der Beweis führt über den Quotientenkörper $K = Quot(R)$. Da $K[X]$ ein Hauptidealring ist wegen Satz 3.8.5, ist er auch faktoriell. Die kanonische Einbettung von R nach K liefert eine Einbettung von $R[X]$ nach $K[X]$. Allerdings muß man nun überlegen, wie man aus Primfaktorzerlegungen in $K[X]$ solche in $R[X]$ erhalten kann. Sei $p \in R$ prim. Man betrachte die Abbildung (Bewertung) $\nu_p \colon R \to \mathbb{N} \cup \{\infty\}$,

$$x \mapsto \sup\{n \in \mathbb{N} \mid p^n \mid x\}.$$

Definition 3.23 (Primbewertungen auf Quotientenkörpern)**.** Sei R ein faktorieller Ring mit Quotientenkörper K und $p \in R$ prim. Man setze die Abbildung ν_p auf K fort durch

$$\nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b) \in \mathbb{Z} \cup \{\infty\}$$

für eine Klasse $\frac{a}{b} \in K$. Für $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ definiere man

$$\nu_p(f) = \min\{\nu_p(a_i) \mid i = 0, \ldots, n\}.$$

Bemerkung 3.9.1. Für $f \in K[X]$ gilt $f \in R[X] \subseteq K[X]$ genau dann, wenn $\nu_p(f) \geq 0$ für alle Primelemente $p \in R$.

Lemma 3.9.2 (Lemma von Gauß)**.** *Sei R ein faktorieller Ring mit Quotientenkörper K und $p \in R$ prim. Dann gilt für alle $f, g \in K[X]$*

$$\nu_p(fg) = \nu_p(f) + \nu_p(g).$$

Sind zudem f, g beide normiert und $fg \in R[X]$, so folgt $f, g \in R[X]$.

Beweis. 1. Die "Gradgleichung"gilt offensichtlich für $f, g \in K$, wie man leicht mit der Primfaktorzerlegung von Zähler und Nenner nachrechnet.

2. Sei $S = \{0, 1, \ldots, n\}$. Ist $f \in K$ und $g = \sum_{j=0}^{n} b_j X^j \in K[X]$, so folgt

$$\begin{aligned}
\nu_p(fg) &= \nu_p\left(\sum_{j=0}^{n} f b_j X^j\right) \\
&= \min\{\nu_p(f b_j) \mid j \in S\} \\
&= \min\{\nu_p(f) + \nu_p(b_j) \mid j \in S\} \\
&= \nu_p(f) + \min\{\nu_p(b_j) \mid j \in S\} \\
&= \nu_p(f) + \nu_p(g).
\end{aligned}$$

3. Wir zeigen nun, dass die Gradformel für $f, g \in R[X]$ mit $\nu_p(f) = \nu_p(g) = 0$ gilt. Die natürliche Projektion $R \to R/(p)$ induziert einen Ringhomomorphismus

$$\pi\colon R[X] \to R/(p)[X].$$

Da p prim ist, ist (p) ein Primdeal in R und daher $R/(p)$ ein Integritätsring, wegen Satz 3.6.2. Nach Korollar 3.5.2 ist dann auch $R/(p)[X]$ ein Integritätsring. Nach Konstruktion gilt

$$\ker(\pi) = \{h \in R[X] \mid \nu_p(h) > 0\}.$$

Wegen $\nu_p(f) = \nu_p(g) = 0$ gilt $\pi(f), \pi(g) \neq 0$. Da $R/(p)[X]$ nullteilerfrei ist, folgt $\pi(fg) \neq 0$, also $fg \notin \ker(\pi)$, und deshalb $\nu_p(fg) = 0$. Damit gilt die Gradgleichung auch in diesem Fall.

4. Nun können wir den allgemeinen Fall behandeln. Seien $f, g \in K[X]$. Dann gibt es Elemente $c, d \in K^\times$ mit $cf, dg \in R[X]$ und $\nu_p(cf) = \nu_p(dg) = 0$. Man kann zum Beispiel mit dem Produkt aller Nenner multiplizieren und durch geeignete p-Potenzen dividieren. Mit den vorangegangenen Fällen folgt nun

$$\begin{aligned}
\nu_p(cd) + \nu_p(fg) &\overset{2.}{=} \nu_p(cdfg) \\
&= \nu_p(cf \cdot dg) \\
&\overset{3.}{=} \nu_p(cf) + \nu_p(dg) \\
&\overset{2.}{=} \nu_p(c) + \nu_p(f) + \nu_p(d) + \nu_p(g) \\
&\overset{1.}{=} \nu_p(cd) + \nu_p(f) + \nu_p(g).
\end{aligned}$$

Das ergibt die Behauptung.

Da f, g normiert sind, folgt $\nu_p(f), \nu_p(g) \leq 0$, und fg ist ebenfalls normiert. Da die Koeffizienten von fg sogar in R liegen, gilt $\nu_p(fg) = 0$. Also liefert die Gradgleichung

$$0 = \nu_p(fg) = \nu_p(f) + \nu_p(g),$$

und somit $\nu_p(f) = \nu_p(g) = 0$. Da dies für alle Primelemente p gilt, folgt, dass in f und g keine echten Nenner auftreten können. Also gilt $f, g \in R[X]$. □

Definition 3.24. Sei R ein faktorieller Ring. Ein Polynom f in $R[X]$ heißt *primitiv*, wenn $\nu_p(f) = 0$ für alle Primelemente $p \in R$ gilt.

Bemerkung 3.9.3. Ist $f \in R[X]$, so heißt

$$c(f) = \prod_p p^{\nu_p(f)}$$

der *Inhalt* von f. Dabei läuft das Produkt über ein Repräsentantensystem von Primelementklassen, mit genau einem Primelement in der Äquivalenzklasse bezüglich Assoziiertheit. Ein Polynom f ist genau dann primitiv, wenn sein Inhalt 1 ist.

Lemma 3.9.4. *Sei R ein faktorieller Ring mit Quotientenkörper K. Dann gelten die folgenden Aussagen.*

(1) Ist $q \in R$ prim in R, so auch in $R[X]$.

(2) Ist $q \in R[X]$ primitiv und prim in $K[X]$, so ist q schon prim in $R[X]$.

(3) Jedes Polynom $f \neq 0$, f keine Einheit in $R[X]$ ist ein Produkt von Primelementen von R und von primitiven Polynomen in $R[X]$, die prim in $K[X]$ sind.

Beweis. Zu (1). Wie wir im Beweis von Lemma 3.9.2 gesehen haben, ist $R/(q)[X]$ ein Integritätsring, da q prim in R ist. Der kanonische Ringhomomorphismus

$$R[X]/(q) \to R/(q)[X],$$

der $r + qR[X]$ auf $r + qR$ abbildet für $r \in R$, und $[X]$ auf X, zeigt, dass auch $R[X]/(q)$ ein Integritätsring ist. Also ist das von q erzeugte Ideal in $R[X]$ prim. Dann ist q prim in $R[X]$ wegen Lemma 3.8.2.

Zu (2). Sei $q \in R[X]$ primitiv und prim in $K[X]$. Seien $f, g \in R[X]$ mit $q \mid fg$. Dann ist q auch auch in $K[X]$ ein Teiler von fg. Da q prim in $K[X]$ ist, ist q ein Teiler von f oder g in $K[X]$. Ohne Einschränkung gelte $q \mid f$, d.h., es gibt ein $h \in K[X]$ mit $f = qh$. Da q primitiv ist und wegen Lemma 3.9.2 gilt

$$\begin{aligned} \nu_p(h) &= \nu_p(qh) - \nu_p(q) \\ &= \nu_p(f) - \nu_p(q) \\ &= \nu_p(f) \geq 0. \end{aligned}$$

Also ist $h \in R[X]$, siehe Bemerkung 3.9.1. Insbesondere ist q ein Teiler von f in $R[X]$. Somit ist q prim in $R[X]$.

Zu (3). Sei $f \neq 0$ in $R[X]$. Wir dürfen annehmen, dass f primitiv ist. Ansonsten multiplizieren wir den größten gemeinsamen Teiler der Koeffizienten von f aus und erhalten eine Zerlegung $f = cg$ mit $c \neq 0$ in R und einem primitiven Polynom $g \in R[X]$. Da R faktoriell ist, besitzt c eine Primfaktorzerlegung in R, wenn es nicht eine Einheit ist. Nach (1) ist eine solche Primfaktorzerlegung von c auch eine in $R[X]$. Sei also f jetzt primitiv mit $\deg(f) > 0$. Der Ring $K[X]$ ist als Hauptidealring über einem Körper faktoriell. Aufgefasst als Element von $K[X]$ besitzt f somit eine Primfaktorzerlegung der Form $f = p_1 \cdots p_n$ mit Primelementen $p_i \in K[X]$. Indem wir mit den Nennern der Koeffizienten dieser Polynome multiplizieren und jeweils durch den größten gemeinsamen Teiler der entstehenden Koeffizienten dividieren, erhalten wir $c_1, \ldots, c_n \in R \setminus 0$ und primitive Polynome $q_1, \ldots, q_n \in R[X]$ mit

$$f = \frac{q_1}{c_1} \cdots \frac{q_n}{c_n} = \frac{1}{c} \cdot q_1 \cdots q_n,$$

wobei $c = \frac{1}{c_1} \cdots \frac{1}{c_n}$. Da f und alle q_i primitiv sind, folgt aus Lemma 3.9.2

$$\begin{aligned}\nu_p(c) &= \nu_p(f) - \sum_{i=1}^{n} \nu_p(q_i) \\ &= 0\end{aligned}$$

für alle Primelemente p in R. Also folgt $c \in R$. Da $\frac{1}{c} = c_1 \cdots c_n$ ist sogar $c \in R^\times$. Also ist

$$f = (cq_1) \cdots q_2 \cdots q_n$$

eine Faktorisierung der gewünschten Form. □

Aus diesem Lemma erhalten wir insbesondere, dass jedes nicht-triviale Element in $R[X]$ eine Primfaktorzerlegung besitzt. Also ist $R[X]$ faktoriell.

Theorem 3.9.5 (Satz von Gauß)**.** *Sei R ein faktorieller Ring. Dann ist auch $R[X]$ faktoriell.*

Beispiel 3.9.6. *Der Polynomring $(\mathbb{Z}[i])[X]$ ist faktoriell.*

In der Tat ist $\mathbb{Z}[i]$ Euklidisch, also ein Hauptidealring und ein faktorieller Ring.

Korollar 3.9.7. *Sei R ein faktorieller Ring mit Quotientenkörper K und sei $f \in R[X]$ ein primitives Polynom. Dann sind die folgenden Aussagen äquivalent.*

(1) Das Polynom f ist prim in $R[X]$.

(2) Das Polynom f ist irreduzibel in $R[X]$.

(3) Das Polynom f ist prim in $K[X]$.

(4) Das Polynom f ist irreduzibel in $K[X]$.

Beweis. In faktoriellen Ringen sind die Begriffe prim und irreduzibel nach Korollar 3.8.11 äquivalent. Der Ring $R[X]$ ist in der Tat faktoriell nach dem Satz von Gauss. Ebenso ist $K[X]$ ein faktorieller Ring. Also gelten (1) $\Leftrightarrow$ (2) und (3) $\Leftrightarrow$ (4).

(3) $\Leftrightarrow$ (1): Das folgt aus Lemma 3.9.4, (2).

(1) $\Leftrightarrow$ (3): Die Primfaktorzerlegung von f in $R[X]$ besteht, wie wir gesehen haben, aus Primelementen von R und primitiven Polynomen in $R[X]$, die prim in $K[X]$ sind. Da f in $R[X]$ prim ist, besteht diese Produktzerlegung aus nur einem Faktor. Da f primitiv ist, ist f kein Primelement von R. Also muß f ein Primelement von $K[X]$ sein. □

Bemerkung 3.9.8. Sei R ein faktorieller Ring. Der Satz von Gauß impliziert induktiv, dass auch der iterierte Polynomring $R[X_1, \ldots, X_n]$ ein faktorieller Ring ist. Hierbei ist $R[X_1, X_2] = (R[X_1])[X_2]$, und

$$R[X_1, \ldots, X_k] = (R[X_1, \ldots, X_{k-1}])[X_k]$$

für alle $k \geq 2$.

3.10 Irreduzibilitätskriterien für Polynome

Kriterien, die in gewissen Fällen die Irreduzibilität von Polynomen zeigen, sind unter anderem nützlich wegen der folgenden Konstruktion von neuen Körpern.

Satz 3.10.1. *Sei K ein Körper und $f \in K[X]$ ein irreduzibles Polynom. Dann ist der Restklassenring*

$$K[X]/(f)$$

ein Körper.

Beweis. Wegen Satz 3.8.5 ist $R = K[X]$ ein Hauptidealring. Aus Lemma 3.8.2 folgt, dass (f) ein maximales Ideal in R ist, da f irreduzibel ist. Wegen Satz 3.6.2, Teil (2) ist der Restklassenring $R/(f)$ deshalb ein Körper. □

Beispiel 3.10.2. *Das Polynom $X^2 + 1$ ist irreduzibel in $\mathbb{R}[X]$. Der Restklassenring ist isomorph zu $\mathbb{C}$,*

$$\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}.$$

Die Auswertungsabbildung $\mathbb{R}[X] \to \mathbb{C}$ mit $f \mapsto f(i)$ ist ein surjektiver Ringhomomorphismus, dessen Kern das Ideal ist, welches von dem Minimalpolynom von i erzeugt wird, also von $X^2 + 1$. Hierbei ist $\mathbb{R}[X]$ Euklidisch, also ein Hauptidealring. Deswegen folgt $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$ nach dem ersten Isomorphiesatz.

Bemerkung 3.10.3. Im allgemeinen ist $R[X]/(f)$ kein Körper, auch wenn f irreduzibel in R ist. Es gilt $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$, siehe Beispiel 3.8.3, welches kein Körper ist. Aber X ist irreduzibel in $\mathbb{Z}[X]$.

Theorem 3.10.4 (Nullstellenkriterium)**.** *Sei K ein Körper und $f \in K[X]$ mit* $\deg(f) > 1$. *Hat f eine Nullstelle in K, so ist f reduzibel in $K[X]$. Hat f Grad 2 oder 3, so ist f genau dann irreduzibel, wenn f keine Nullstelle in K hat.*

Beweis. Polynomdivision von f durch $X - a$ ergibt $f = q(X - a) + r$ mit eindeutig bestimmten $q, r \in K[X]$ und $\deg(r) < 1$. Nach Voraussetzung folgt $0 = f(a) = r$ und $f = (X - a)q$ ist in $K[X]$ reduzibel.
Für die zweite Behauptung nehme man an, f sei reduzibel. Also existieren $g, h \in K[X]$ mit $f = gh$, und g, h sind nicht Null und keine Einheiten in $K[X]$. Insbesondere ist $\deg(g) > 0$ und $\deg(h) > 0$. Wegen

$$\deg(g) + \deg(h) = \deg(gh) = \deg(f) \in \{2, 3\}$$

ist einer der beiden Grade gleich 1. Ohne Einschränkung sei $\deg(g) = 1$. Also ist $g = aX + b$ mit $a \neq 0$, und somit $f(-b/a) = g(-b/a)h(-b/a) = 0$. Also hat f eine Nullstelle in K. □

Für Polynome von Grad $n \geq 4$ gilt die Aussage im allgemeinen nicht mehr. So hat $f = (x^2 + 1)^2$ keine Nullstellen in $\mathbb{R}[X]$, ist aber reduzibel.

Korollar 3.10.5. *Sei K ein Körper und $f \in K[X]$ mit $f \neq 0$. Dann hat f höchstens* $\deg(f)$ *Nullstellen in K.*

Beweis. Sind $a_1, \ldots, a_n$ Nullstellen von f, dann folgt induktiv aus der Polynomdivision, dass

$$(X - a_1) \cdots (X - a_n) \mid f$$

gilt, wobei der Fall $n = 1$ im Beweis von 3.10.4 gezeigt wurde. Also gilt $n \leq \deg(f)$. □

Bemerkung 3.10.6. Die Aussage von Korollar 3.10.5 gilt auch für Polynome in $R[X]$, wobei R ein Integritätsring ist, aber nicht notwendig ein Körper. Zwar muß dann $R[X]$ kein Euklidischer Ring sein, aber die Polynomdivision für normierte Polynome gilt in jedem Ring R, siehe Satz 3.5.3. Damit kann man den Beweis mit Induktion auch für $R[X]$ machen. Allerdings benötigt man, dass R keine Nullteiler hat. Ist $f(a) = 0$ und $f = (X - a)q + f(a)$ mit $b \neq a$ und $f(b) = 0$, dann hat man $0 = f(b) = (b - a)q(b)$ und man möchte $q(b) = 0$ schließen für den Induktionsschritt. In der Tat, wenn R Nullteiler hat, so wird die Aussage falsch:

$$f = X^2 - 1$$

hat 4 Nullstellen in $R = \mathbb{Z}/8\mathbb{Z}$.

Sei f ein reduzibles Polynom in $R[X]$. Dann hat man $f = gh$ mit $g, h \in R[X]$. Im allgemeinen kann man nicht schliessen, dass $\deg(g) > 0$ und $\deg(h) > 0$ gilt. Zum Beispiel ist $f = 2(X + 1) \in \mathbb{Z}[X]$ reduzibel, weil 2 keine Einheit ist. Ist f allerdings primitiv, also etwa ein normiertes Polynom, so folgt die Aussage. Das werden wir im Beweis des folgenden Resultates brauchen.

Theorem 3.10.7 (Reduktionskriterium)**.** *Sei R ein faktorieller Ring mit Quotientenkörper K, p ein Primelement in R und $\pi\colon R[X] \to R/(p)[X]$ der von der kanonischen Projektion $R \to R/(p)$ induzierte Ringhomomorphismus. Sei $f \in R[X]$ ein Polynom vom Grad* $\deg(f) > 0$*, dessen Leitkoeffizient nicht durch p teilbar ist. Dann gelten folgende Aussagen.*

(1) Ist f primitiv und $\pi(f)$ in $R/(p)[X]$ irreduzibel, so ist f in $R[X]$ irreduzibel.

(2) Ist $\pi(f)$ in $R/(p)[X]$ irreduzibel, so ist f in $K[X]$ irreduzibel.

Beweis. Zu (1): Angenommen, f ist reduzibel in $R[X]$, d.h., $f = gh$, wobei $g, h \in R[X]$ und weder f noch g ein Einheit ist. Da f primitiv ist, können g und h keine Konstanten sein. Also gilt $\deg(f) > 0$ und $\deg(g) > 0$. Dann ist das Produkt der höchsten Koeffizienten von g und h gerade der höchste Koeffizient von f. Da dieser nicht von p geteilt wird, werden auch die höchsten Koeffizienten von g und h nicht von p geteilt. Denn R und $R/(p)$ sind Integritätsringe, so dass $\deg(gh) = \deg(g) + \deg(h)$ und $\deg(\pi(g)\pi(h)) = \deg(\pi(g)) + \deg(\pi(h))$ gilt. Also ist $\deg(\pi(g)) = \deg(g) > 0$ und $\deg(\pi(h)) = \deg(h) > 0$ in $R/(p)[X]$. Wegen

$$\pi(f) = \pi(gh) = \pi(g)\pi(h)$$

ist also $\pi(f)$ in $R/(p)[X]$ reduzibel, Widerspruch. Also ist f irreduzibel in $R[X]$.

Zu (2): Wir können $f = c \cdot g$ schreiben, wobei $c \in R$ der ggT der Koeffizienten von f ist und g dann primitiv ist. Da $\pi(f)$ irreduzibel in $R/(p)[X]$ ist, gilt das erst recht für $\pi(g)$. Nach (1) ist g also irreduzibel in $R[X]$. Nach Korollar 3.9.7 ist g dann auch irreduzibel in $K[X]$. Da K ein Körper ist, ist c aber eine Einheit in $K[X]$. Also ist auch f irreduzibel in $K[X]$. □

Beispiel 3.10.8. *Das Polynom $f = -8X^3 - 4X + 1 \in \mathbb{Z}[X]$ ist irreduzibel in $\mathbb{Z}[X]$ (und in $\mathbb{Q}[X]$).*

In der Tat, Reduktion modulo $p = 3$ in $R = \mathbb{Z}$ liefert das Polynom $\pi(f) = X^3 - X + 1 \in \mathbb{F}_3[X]$, das keine Nullstelle in $\mathbb{F}_3$ hat. Also ist $\pi(f)$ irreduzibel in $\mathbb{F}_3[X]$ nach dem Nullstellenkriterium. Da f primitiv ist, folgt die Behauptung aus dem Reduktionskriterium.

Man kann das folgende Kriterium anwenden, um zu sehen, dass gewisse Polynome keine rationalen Nullstellen haben.

Satz 3.10.9 (Rationaler Nullstellentest)**.** *Sei $f = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ ein Polynom vom Grad n und $a = \frac{r}{s}$ eine rationale Nullstelle von f mit $\gcd(r, s) = 1$. Dann gilt $r \mid a_0$ und $s \mid a_n$ in $\mathbb{Z}$.*

Beweis. Wir dürfen annehmen, dass f primitiv ist, indem wir den ggT herausziehen. Damit ändert man nicht die Menge der rationalen Nullstellen und die Teilbarkeitbedingungen gelten erst recht. Wegen $f\left(\frac{r}{s}\right) = 0$ ist $sX - r$ ein Teiler von f in $\mathbb{Q}[X]$. Nach dem Lemma von Gauss ist dann $f = (sX - r)g$ mit einem primitiven Polynom $g \in \mathbb{Z}[X]$. Jedes Vielfache von $sX - r$ in $\mathbb{Z}[X]$ hat aber einen Leitkoeffizienten, der durch s teilbar ist, und einen konstanten Term, der durch r teilbar ist, also insbesondere auch f. □

Beispiel 3.10.10. *Das Polynom $f = 2X^3 + X - 1$ hat keine rationalen Nullstellen.*

Sei $\frac{r}{s}$ eine Nullstelle von f. Dann gilt $r \mid -1$ und $s \mid 2$. Also sind die potentiellen rationalen Nullstellen gerade ± 1 und $\pm\frac{1}{2}$. Doch keine davon ist eine Nullstelle, wie man leicht ausrechnet.

Bemerkung 3.10.11. Das Reduktionskriterium ist zwar oft recht hilfreich, hat aber auch seine Grenzen. Zum Beispiel ist das Polynom $f = X^4 + 1$ irreduzibel in $\mathbb{Z}[X]$, aber reduzibel über $\mathbb{F}_p$ für *jede* Primzahl p.

Theorem 3.10.12 (Eisensteinsches Irreduzibiliätskriterium)**.** *Sei R ein faktorieller Ring mit Quotientenkörper K und $f = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ ein primitives Polynom vom Grad n. Sei p ein Primelement in R mit $p \mid a_0, \ldots a_{n-1}$ und $p \nmid a_n$, $p^2 \nmid a_0$. Dann ist f irreduzibel in $R[X]$ und $K[X]$.*

Beweis. Wegen Korollar 3.9.7 genügt es zu zeigen, dass f irreduzibel in $R[X]$ ist. Angenommen, $f = gh$ ist reduzibel, mit $g, h \in R[X]$ und $\deg(g) > 0$, $\deg(h) > 0$. Sei $g = b_r X^r + \cdots + b_0$ und $h = c_s X^s + \cdots + c_0$ mit $b_r, c_s \neq 0$. Es gilt

$$r + s = \deg(g) + \deg(h) = \deg(f) = n,$$

da R ein Integritätsring ist. Wegen $r, s > 0$ folgt auch $r, s < n$. Wir haben $a_n = b_r c_s$ und $a_0 = b_0 c_0$. Da $p \nmid a_n$ folgt $p \nmid b_r, c_s$ und da $p^2 \nmid a_0$ teilt p genau eines der Elemente b_0 und c_0. Ohne Einschränkung gelte $p \mid b_0$, $p \nmid c_0$. Sei t maximal mit der Eigenschaft, daß $p \mid b_i$ für alle i mit $0 \leq i \leq t$. Dann ist

$$a_{t+1} = b_{t+1}c_0 + (b_t c_1 + \cdots + b_0 c_{t+1})$$

und jeder Summand in der Klammer ist durch p teilbar, aber nicht der Term $b_{t+1}c_0$. Also ist a_{t+1} nicht durch p teilbar. Nach Voraussetzung geht das nur für $t+1 = n$. Aber dann ist $r = \deg(g) \geq t+1 = n$, im Widerspruch zu $r < n$. □

Beispiel 3.10.13. *Sei $f = X^n - p \in \mathbb{Z}[X]$ mit p prim und $n \geq 1$. Dann ist f irreduzibel in $\mathbb{Z}[X]$ und $\mathbb{Q}[X]$. Insbesondere ist $\sqrt[n]{p}$ irrational.*

Das folgt aus Eisenstein mit der Primzahl p in $\mathbb{Z}$. Manchmal kann man Eisenstein nicht direkt anwenden, sondern erst nach einer Substitution $X \mapsto X + a$. Eine echte Zerlegung von $f(X)$ induziert eine von $f(X+a)$ und umgekehrt, also ändert sich an der Irreduzibilität nichts.

Beispiel 3.10.14. *Sei p ein Primzahl. Das Kreisteilungspolynom*

$$\frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1 \in \mathbb{Z}[X]$$

ist irreduzibel in $\mathbb{Q}[X]$.

Hier können wir Eisenstein nicht direkt anwenden. Wir können aber zeigen, dass $f(X+1)$ irreduzibel ist, und daher auch $f(X)$. Wir haben

$$\begin{aligned} f(X+1) &= \frac{(X+1)^p - 1}{X} \\ &= \frac{1}{X}((X+1)^p - 1) \\ &= X^{p-1} + \binom{p}{1} X^{p-2} + \cdots + \binom{p}{p-1}. \end{aligned}$$

Hier können wir Eisenstein mit der Primzahl p anwenden, da $p \mid \binom{p}{k}$ für $k = 1, \ldots, p-1$ und $p^2 \nmid \binom{p}{p-1} = p$ gilt.

Bemerkung 3.10.15. Es gibt irreduzible Polynome in $\mathbb{Z}[X]$ wie etwa $f = X^4 + 10X^2 + 1$ oder $f = X^3 + X + 1$, auf die man Eisenstein für keine Translation anwenden kann.

4 Körper

4.1 Grundlagen

Wir wiederholen nochmals die Definition eines Körpers, siehe Bemerkung 3.1.2.

Definition 4.1. Ein Körper K ist ein kommutativer Ring mit 1, der nicht der Nullring ist und der $K^\times = K \setminus 0$ erfüllt.

Ein Körperhomomorphismus ist ein Ringhomomorphismus zwischen Körpern. Die Charakteristik von K ist $char(K)$ für K als Ring, im Sinne von Definition 3.8.

Beispiel 4.1.1. *Klassische Beispiele von Körpern sind:*

1. Die Körper $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ der rationalen, reellen und komplexen Zahlen der Charakteristik Null.

2. Der endliche Körper $\mathbb{F}_p$ der Charakteristik $p > 0$, mit p prim.

3. Der unendliche Körper $\mathbb{F}_p(X) = Quot(\mathbb{F}_p[X])$ der Charakteristik p.

Satz 4.1.2. *Jeder Homomorphismus $f\colon K \to L$ von Körpern ist injektiv.*

Beweis. Jeder Körper K hat genau zwei Ideale, nämlich 0 und K. Also ist entweder $\ker(f) = 0$, oder $\ker(f) = K$. Wegen $f(1) = 1 \neq 0$ ist die zweite Möglichkeit ausgeschlossen. Also ist f injektiv. □

Satz 4.1.3. *Sei K ein Körper und $G \leq K^\times$ eine endliche Untergruppe der Einheitengruppe von K. Dann ist G zyklisch.*

Beweis. Nach dem Klassifikationssatz endlicher abelscher Gruppen, Theorem 2.7.6 gilt

$$G \cong \prod_{j=1}^{k} C_{p_j^{n_j}}$$

mit Primzahlen $p_1, \ldots, p_k$ und $|G| = n = p_1^{n_1} \cdots p_k^{n_k}$. Sei

$$m = lcm(p_1^{n_1}, \ldots, p_k^{n_k}).$$

Offenbar gilt $m \leq n$. Ist $a_i \in C_{p_i^{n_i}}$, dann folgt $a_i^{p_i^{n_i}} = 1$ in multiplikativer Schreibweise, also $a_i^m = 1$. Somit gilt $a^m = 1$ für alle $a \in G$, und jedes Element von G ist eine Nullstelle von $X^m - 1$. Da das Polynom höchstens m Nullstellen in K haben kann, folgt $n \leq m$ und daher $m = n$. Nun folgt $G \cong \mathbb{Z}/n\mathbb{Z}$ nach dem Chinesischen Restsatz. □

Korollar 4.1.4. *Sei K ein endlicher Körper mit p^n Elementen. Dann ist die Gruppe $K^\times$ zyklisch und isomorph zu C_{p^n-1}.*

Lemma 4.1.5. *Sei R ein Integritätsring der Charakteristik p, mit p prim. Dann gilt für alle $a, b \in R$ und $r \in \mathbb{N}$*

$$\begin{aligned}(a+b)^{p^r} &= a^{p^r} + b^{p^r},\\ (a-b)^{p^r} &= a^{p^r} - b^{p^r}.\end{aligned}$$

Beweis. Die Identitäten folgen mit Induktion über $r \geq 1$. Der Schluß von $r \to r+1$ ist klar. Für $r = 1$ haben wir, weil p ein Teiler von $\binom{p}{k}$ ist für $k = 1, \ldots, p-1$,

$$\begin{aligned}(a+b)^p &= a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{n-k} b^k + b^p\\ &= a^p + b^p\end{aligned}$$

in R. Ersetzt man b durch $-b$, so ist $(a+(-b))^p = a^p + (-b)^p = a^p + b^p$ für alle $p > 2$. Ist p gerade, so folgt $p = 2$ und $-1 = 1$. Damit ist der Fall $r = 1$ bewiesen. □

Definition 4.2. Sei K ein Körper der Charakteristik p. Dann ist die Abbildung $\sigma\colon K \to K, a \mapsto a^p$ ein Homomorphismus von Körpern, siehe Lemma 4.1.5. Er heißt *Frobenius-homomorphismus* von K.

4.2 Körpererweiterungen

Definition 4.3. Sei L ein Körper. Ein *Teilkörper* K von L ist ein Unterring von L, so dass K mit jedem Element ungleich Null auch sein multiplikatives Inverses enthält. Dann ist $K \subseteq L$ selbst ein Körper bezüglich Addition und Multiplikation von L. Man nennt L eine *Körpererweiterung* on K und schreibt $L \mid K$. Ein *Zwischenkörper* der Erweiterung $L \mid K$ ist ein Teilkörper M von L mit $K \subseteq M \subseteq L$.

Beispiel 4.2.1. *1. $\mathbb{C} \mid \mathbb{C}$, $\mathbb{C} \mid \mathbb{R}$ und $\mathbb{C} \mid \mathbb{Q}$ sind Körpererweiterungen.*

2. $\mathbb{Q}(i)$ is ein Zwischenkörper der Erweiterung $\mathbb{C} \mid \mathbb{Q}$.

Definition 4.4. Sei $L \mid K$ eine Körpererweiterung und $S \subseteq L$ eine Teilmenge. Mit $K(S)$ wird der kleinste Teilkörper von L bezeichnet, der S enthält. Er ist der Durchschnitt aller Zwischenkörper von $L \mid K$, die S enthalten. Man sagt auch, das $K(S)$ durch *Adjunktion* von S in $L \mid K$ zu K entsteht.

Ist $S = \{\alpha_1, \ldots, \alpha_n\}$, so schreibt man auch $K(S) = K(\alpha_1, \ldots, \alpha_n)$. In $\mathbb{C} \mid \mathbb{Q}$ ist $K(S)$ mit $S = \{i\}$ also durch $\mathbb{Q}(i)$ gegeben. Ist $S = \{\zeta_n\}$, wobei ζ_n eine Einheitswurzel in $\mathbb{C}$ ist, d.h., eine Nullstelle von $X^n - 1$ in $\mathbb{C}$, so ist $K(S) = \mathbb{Q}(\zeta_n)$.

Definition 4.5. Seien M, N zwei Zwischenkörper in einer Körpererweiterung $L \mid K$. Dann bezeichnet $MN = K(M \cup N)$ das *Kompositum* von M und N in $L \mid K$.

Seien ζ_m und ζ_n Einheitswurzeln in $\mathbb{C}$. Die Körper $\mathbb{Q}(\zeta_m)$ und $\mathbb{Q}(\zeta_n)$ heißen *Kreisteilungskörper.*

Beispiel 4.2.2 (Übungsaufgabe)**.** *Seien $m, n \in \mathbb{N}$ und $[m, n]$ das kgV von m und n. Dann gilt für das Kompositum von $\mathbb{Q}(\zeta_m)$ und $\mathbb{Q}(\zeta_n)$ in $\mathbb{C} \mid \mathbb{Q}$,*

$$\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{[m,n]}).$$

Bemerkung 4.2.3. Für $S = \{\alpha_1, \ldots, \alpha_n\}$ enthält $K(S)$ den Ring

$$K[S] := \{f(\alpha_1, \ldots, \alpha_n) \mid f \in K[X_1, \ldots, X_n]\}$$

aller polynomialen Ausdrücke $f(\alpha_1, \ldots, \alpha_n)$ in den α_i mit Koeffizienten in K. Es gilt $K(S) = Quot(K[S])$.

Definition 4.6. Der kleinste Teilkörper P in einem Körper K wird der *Primkörper* genannt. Er ist der Schnitt aller Teilkörper von K.

Satz 4.2.4. *Sei K ein Körper und P sein Primkörper. Hat K Charakteristik Null, so gilt $P \cong \mathbb{Q}$, und hat K Charakteristik p, so gilt $P \cong \mathbb{F}_p$.*

Beweis. Die Abbildung $\varphi\colon \mathbb{Z} \to P$, $n \mapsto n \cdot 1$ ist ein Ringhomomorphismus mit $\mathrm{im}(\varphi) \cong \mathbb{Z}/\ker(\varphi)$. Gilt $char(K) = 0$, so ist $\mathrm{im}(\varphi) \cong \mathbb{Z}$, und P enthält mit $\mathrm{im}(\varphi)$ auch

$$Quot(\mathrm{im}(\varphi)) \cong \mathbb{Q}.$$

Wegen der Minimalität von P folgt $P \cong \mathbb{Q}$. Gilt $char(K) = p$, so ist $\mathrm{im}(\varphi) \cong \mathbb{Z}/p\mathbb{Z}$ und daher $P \cong \mathbb{F}_p$. □

Ist $L \mid K$ eine Körpererweiterung, so ist L bezüglich der Multiplikation mit Elementen aus K insbesondere ein K-Vektorraum und besitzt somit eine Dimension über K.

Definition 4.7. Eine Erweiterung $L \mid K$ heißt *endlich erzeugt*, falls es Elemente $\alpha_1, \ldots, \alpha_n \in L$ gibt mit $L = K(\alpha_1, \ldots, \alpha_n)$. Sie heißt *einfach*, wenn es ein $\alpha \in L$ gibt mit $L = K(\alpha)$. Ein solches α, welches nicht eindeutig sein muss, heißt *primitives Element.* Der *Grad* einer Erweiterung $L \mid K$ ist definiert als

$$[L : K] := \dim_K(L).$$

Die Erweiterung heißt *endlich*, falls $[L : K] < \infty$ gilt.

Beispiel 4.2.5. *1. Die Erweiterung $K \mid K$ hat Grad* 1.

2. Die Erweiterung $\mathbb{C} \mid \mathbb{R}$ hat Grad 2.

3. Die Erweiterung $\mathbb{Q}(i) \mid \mathbb{Q}$ hat Grad 2.

4. Die Erweiterung $\mathbb{C} \mid \mathbb{Q}$ ist unendlich.

Eine Vektorraumbasis von $\mathbb{C}$ über $\mathbb{R}$ ist $\{1, i\}$. Das gilt auch für $\mathbb{Q}(i) \mid \mathbb{Q}$. Es gilt $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$. Aber $\mathbb{Q}(\sqrt[3]{2}) \neq \{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\}$.

Analog zum Index von Untergruppen in der Gruppentheorie gilt folgendes Resultat.

Satz 4.2.6 (Gradsatz)**.** *Sei $L \mid K$ eine Körpererweiterung und sei M ein Zwischenkörper von $L \mid K$. Dann gilt*

$$[L : K] = [L : M] \cdot [M : K]$$

Der Grad $[L : K]$ ist genau dann unendlich, wenn einer der Grade $[L : M]$ oder $[M : K]$ unendlich ist.

Beweis. Sei $(b_i)_{i \in I}$ eine Basis von $M \mid K$ und $(c_i)_{i \in J}$ eine Basis von $L \mid M$. Dann ist die Familie $(b_i c_j)_{i,j} \in I \times J$ in L linear unabhängig über K und ein Erzeugendensystem, und damit eine Basis von $L \mid K$. Also ist

$$\begin{aligned}[L : K] &= \dim_K(L) \\ &= |I \times J| \\ &= |I| \cdot |J| \\ &= [L : M] \cdot [M : K].\end{aligned}$$

□

Korollar 4.2.7. *Sind $L \mid M \mid K$ Körpererweiterungen mit $[L : K] = p$ prim, dann gilt $M = L$ oder $M = K$.*

Beweis. Aus $p = [L : M] \cdot [M : K]$ folgt entweder $[L : M] = 1$ oder $[M : K] = 1$. Das bedeutet aber, $L = M$ oder $M = K$. □

Beispiel 4.2.8. *Die Körpererweiterung $\mathbb{C} \mid \mathbb{R}$ hat keinen echten Zwischenkörper.*

Wegen $[\mathbb{C} \colon \mathbb{R}] = 2$ folgt das aus Korollar 4.2.7.

Satz 4.2.9. *Sei $L \mid K$ eine endliche Körpererweiterung. Dann ist $L \mid K$ endlich erzeugt.*

Beweis. Da $L \mid K$ endlich ist, gibt es eine endliches Erzeugendensystem $S \subset L$ von L als K-Vektorraum. Wegen $L = span_K(S) \subseteq K(S) \subseteq L$ folgt dann bereits $L = K(S)$. □

Satz 4.2.10. *Sei $L \mid K$ eine Körpererweiterung mit Zwischenkörpern M und N. Dann ist $[MN : M] \leq [N : K]$, also*

$$[MN : K] \leq [M : K] \cdot [N : K].$$

Sind $[M : K]$ und $[N : K]$ teilerfremd, so gilt die Gleichheit

$$[MN : K] = [M : K] \cdot [N : K].$$

Beweis. Ist $[N : K] = \infty$, so ist nichts zu zeigen. Ist $N \mid K$ endlich, so ist $N \mid K$ endlich erzeugt. Das gleiche gilt für $[M : K]$. Sei also $v_1, \ldots, v_m$ eine Basis von M über K, und $w_1, \ldots, w_n$ eine Basis von N über K. Da MN der kleinste Körper ist, der M und N enthält, gilt

$$\begin{aligned} MN &= K(v_1, \ldots, v_m, w_1, \ldots, w_n) \\ &= M(w_1, \ldots, w_n). \end{aligned}$$

Also ist $[MN : M] \leq n = [N : K]$. Wegen $K \subseteq M \subseteq MN$ folgt aus dem Gradsatz 4.2.6

$$\begin{aligned} [MN : K] &= [MN : M] \cdot [M : K] \\ &\leq [N : K] \cdot [M : K]. \end{aligned}$$

Sind nun $[M : K] = m$ und $[N : K] = n$ teilerfremd, so folgt auch die andere Ungleichung. Da M, N Teilkörper von MN sind, folgt aus dem Gradsatz

$$\begin{aligned} m = [M : K] \mid [MN : K], \\ n = [N : K] \mid [MN : K]. \end{aligned}$$

Damit teilt auch $mn = \frac{mn}{\gcd(m,n)} = \operatorname{lcm}(m, n)$ den Grad $[MN : K]$. Also folgt

$$[MN : K] \geq [M : K] \cdot [N : K].$$

□

Definition 4.8. Sei $L \mid K$ eine Körpererweiterung und $\alpha \in L$. Das Element α heißt *algebraisch* über K, wenn es ein Polynom $f \in K[X]$ gibt, mit $f \neq 0$ und $f(\alpha) = 0$. Andernfalls heißt es *transzendent* über K.

Beispiel 4.2.11. *1. Die Zahl $\sqrt{2}$ ist algebraisch über $\mathbb{Q}$, da $f(\sqrt{2}) = 0$ für $f = X^2 - 2 \in \mathbb{Q}[X]$.*

2. Die Zahl i ist algebraisch über $\mathbb{Q}$ und $\mathbb{R}$, da $f(i) = 0$ für $f = X^2 + 1 \in \mathbb{Q}[X]$.

3. Die Zahlen e und π sind algebraisch über $\mathbb{R}$, mit $f = X - e$ bzw. $f = X - \pi$ in $\mathbb{R}[X]$.

4. Die Zahlen e und π sind transzendent über $\mathbb{Q}$ (Hermite 1873 und Lindemann 1882).

Bemerkung 4.2.12. Da der Polynomring $\mathbb{Q}[X]$ abzählbar ist und jedes Polynom in $\mathbb{Q}[X] \setminus 0$ nur endlich viele Nullstellen in $\mathbb{C}$ besitzt, gibt es in $\mathbb{C}$ nur abzählbar viele über $\mathbb{Q}$ algebraische Zahlen. Also gibt es in $\mathbb{C}$ überabzählbar viele transzendente Zahlen über $\mathbb{Q}$. Von einer gegebenen komplexen Zahl zu entscheiden, ob sie algebraisch oder transzendent über $\mathbb{Q}$ ist, ist im allgemeinen sehr schwer. Zum Beispiel ist nicht bekannt, ob $\frac{e}{\pi}$, oder $e + \pi$ algebraisch über $\mathbb{Q}$ ist oder nicht. Der Satz von Gelfond-Schneider besagt, dass für alle algebraischen Zahlen a, b mit $a \neq 0, 1$ und $b \notin \mathbb{Q}$ die Zahlen a^b transzendent sind. Hierbei ist a^b mehrwertig, nämlich $\exp(b \cdot \log(a))$, und $\log(a)$ ist nur eindeutig bis auf ganzzahlige Vielfache von $2\pi i$. Insbesondere ist

$$e^\pi = (e^{i\pi})^{-i} = (-1)^{-i} \simeq 23.14069$$

transzendent, da -1 und $-i$ algebraisch sind.

Sind $L \mid K$ und $M \mid K$ Körpererweiterungen von K, so ist ein Morphismus von $L \mid K$ nach $M \mid K$ ein Körperhomomorphismus $f\colon L \to M$ mit $f_{|K} = \mathrm{id}_K$. Ein Morphismus von Körperweiterungen über K, der einen bezüglich Komposition inversen Morphismus von Körpererweiterungen besitzt, heißt ein *Isomorphismus von Körpererweiterungen über K.*

Satz 4.2.13. *Sei $L \mid K$ eine Körpererweiterung und $\alpha \in L$. Sei*

$$E_\alpha\colon K[X] \to L,\ f \mapsto f(\alpha)$$

der Einsetzhomomorphismus zu α. Dann gelten folgende Aussagen.

(1) *Das Element α ist genau dann algebraisch, wenn E_α nicht injektiv ist.*

(2) *Ist α transzendent über K, so sind die Körpererweiterungen $K(X)$ und $K(\alpha)$ über K isomorph. Insbesondere gilt*

$$K(\alpha) \cong K(X) = \mathrm{Quot}(K[X]), \quad [K(\alpha) : K] = \infty.$$

(3) *Ist α algebraisch über K, so sind die Körpererweiterungen $K(\alpha)$ und $K[X]/\ker(E_\alpha)$ über K isomorph. Insbesondere gilt*

$$K(\alpha) \cong K[X]/\ker(E_\alpha),$$

und es gibt ein eindeutig bestimmtes normiertes Polynom $\mu_\alpha \in K[X]$ minimalen Grades mit $\mu_\alpha(\alpha) = 0$, das Minimalpolynom *von α über K. Dieses Polynom ist prim und es gilt $\ker(E_\alpha) = (\mu_\alpha)$ sowie*

$$[K(\alpha) : K] = \deg(\mu_\alpha).$$

Beweis. Zu (1): Offenbar ist α genau dann transzendent, wenn $\ker(E_\alpha) = 0$ ist, d.h., $f(\alpha) = 0$ nur für das Nullpolynom gilt.

Zu (2): Da E_α injektiv ist, induziert E_α einen injektiven Körperhomomorphismus $\overline{E_\alpha}\colon K(X) \to L$ mit $\mathrm{im}(\overline{E_\alpha}) = K(\alpha)$. Also ist

$$K(X) \cong K(X)/\ker(\overline{E_\alpha}) \cong \mathrm{im}(\overline{E_\alpha}) = K(\alpha).$$

Zu (3): Nach Voraussetzung ist das Ideal $I = \ker(E_\alpha)$ ungleich Null. Da $K[X]/\ker(E_\alpha) \cong \mathrm{im}(E_\alpha)$ als Unterring des Körpers K ein Integritätsring ist, muss I ein Primideal in $K[X]$ sein. Da $K[X]$ ein Hauptidealring ist, ist I auch ein maximales Ideal. Somit ist $K[X]/I \cong \mathrm{im}(E_\alpha)$ ein Körper. Wegen $\alpha \in \mathrm{im}(E_\alpha) \subseteq K(\alpha)$ gilt $\mathrm{im}(E_\alpha) = K(\alpha)$. Also ist $K[X]/I \cong K(\alpha)$. Das Ideal I ist ein Hauptideal, da $K[X]$ eine Hauptidealring ist. Sein Erzeuger ist bis auf Einheiten von K eindeutig bestimmt. Also gibt es ein eindeutig bestimmtes normiertes Primpolynom $p \in K[X]$ mit $I = (p)$. Division mit Rest zeigt, dass dieses p das eindeutig bestimmte normierte Polynom in $K[X]$ minimalen Grades mit Nullstelle α ist, d.h., mit $p = \mu_\alpha$. Sei $d := \deg(\mu_\alpha)$. Wir zeigen, dass $\{1, \alpha, \ldots, \alpha^{d-1}\}$ eine K-Basis von $K(\alpha)$ ist. Dann ist $[K(\alpha) : K] = \deg(\mu_\alpha)$. Sei also $x \in K(\alpha)$. Wegen

$K(\alpha) \cong K[X]/(\mu_\alpha)$ gibt es ein $g \in K[X]$ mit $g(\alpha) = x$. Division mit Rest von g durch μ_α zeigt, dass wir außerdem g so wählen können, dass $\deg(g) < \deg(\mu_\alpha) = d$ ist. Also ist

$$x = g(\alpha) \in span_K\{1, \alpha, \ldots, \alpha^{d-1}\}.$$

Es bleibt noch zu zeigen, dass $\{1, \alpha, \ldots, \alpha^{d-1}\}$ linear unabhängig über K ist. Gilt

$$\sum_{j=0}^{d-1} \lambda_j \alpha^j = 0$$

für $\lambda_0, \ldots, \lambda_{d-1} \in K$, dann ist α eine Nullstelle des Polynoms

$$f = \sum_{j=0}^{d-1} \lambda_j X^j \in K[X].$$

Aufgrund der Minimalität von μ_α und $\deg(f) \leq d - 1 < \deg(\mu_\alpha)$ folgt, dass $f = 0$ ist. Also ist $\lambda_0 = \cdots = \lambda_{d-1} = 0$. □

Beispiel 4.2.14. *Sei $L = \mathbb{C}$, $K = \mathbb{Q}$ und $\alpha = \sqrt[3]{2}$. Dann ist α algebraisch über K mit $\mu_\alpha = X^3 - 2 \in K[X]$ und $[K(\alpha) : K] = 3$. Also ist $\mathbb{Q}(\sqrt[3]{2}) \neq \{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\}$, siehe Beispiel* 4.2.5.

In der Tat, $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$. Das Polynom $X^3 - 2 \in \mathbb{Q}[X]$ ist irreduzibel, siehe Beispiel 3.10.13 und normiert und daher das Minimalpolynom der Nullstelle $\sqrt[3]{2}$.

Beispiel 4.2.15. *Sei p eine Primzahl und $n \in \mathbb{N}$. Dann ist $\sqrt[n]{p}$ algebraisch über $\mathbb{Q}$ und $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$. Da $\mathbb{R}$ alle Zahlen $\sqrt[n]{p}$ enthält, für n beliebig groß, ist die Körpererweiterung $\mathbb{R} \mid \mathbb{Q}$ unendlich.*

Das Polynom $X^n - p \in \mathbb{Q}[X]$ ist irreduzibel, siehe Beispiel 3.10.13 und normiert und daher das Minimalpolynom der Nullstelle $\sqrt[n]{p}$.

4.3 Algebraische Erweiterungen

Definition 4.9. Sei $L \mid K$ eine Körpererweiterung. Sie heißt *algebraisch*, wenn jedes Element aus L algebraisch über K ist. Sie heißt *transzendent*, wenn sie nicht algebraisch ist, d.h., wenn sie mindestens ein Element enthält, das nicht algebraisch über K ist.

Beispiel 4.3.1. *1. Die triviale Erweiterung $K \mid K$ ist algebraisch.*

2. Die Erweiterung $\mathbb{R} \mid \mathbb{Q}$ ist transzendent, da z.B. π transzendent über $\mathbb{Q}$ ist.

Satz 4.3.2. *Jede endliche Körpererweiterung $L \mid K$ ist algebraisch.*

Beweis. Sei $L \mid K$ eine endliche Körpererweiterung und sei $\alpha \in L$. Dann gilt nach dem Gradsatz

$$[L : K(\alpha)] \cdot [K(\alpha) : K] = [L : K] < \infty,$$

also ist auch die Erweiterung $K(\alpha) \mid K$ endlich, und somit α algebraisch nach Satz 4.2.13. □

Damit erhalten wir viele Beispiele algebraischer Erweiterungen.

Beispiel 4.3.3. *1. Die Erweiterung $\mathbb{Q}(\sqrt[n]{p}) \mid \mathbb{Q}$ ist algebraisch.*

2. Die Erweiterung $\mathbb{C} \mid \mathbb{R}$ ist algebraisch.

3. Die Erweiterung $\mathbb{Q}(\zeta_p) \mid \mathbb{Q}$, für p prim, ist algebraisch.

In 3. ist das Minimalpolynom von ζ_p durch $f = X^{p-1} + \cdots + X + 1$ gegeben. Diese Polynom ist irreduzibel über $\mathbb{Q}$, siehe Beispiel 3.10.14, und hat ζ_p als Nullstelle, wegen $f = \frac{X^p-1}{X-1}$. Also gilt $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ und somit ist die Erweiterung endlich und algebraisch. Das bleibt auch für n-te Einheitswurzeln richtig, für beliebiges n. Es gilt $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$. Dazu fehlt uns aber noch die Bestimmung des Minimalpolynoms von ζ_n über $\mathbb{Q}$.

Algebraische Erweiterungen sind im allgemeinen nicht endlich, siehe Beispiel 4.3.7. Es gilt aber folgender Satz.

Satz 4.3.4. *Sei $L \mid K$ eine Körpererweiterung. Ist $L \mid K$ algebraisch und endlich erzeugt, so ist $L \mid K$ endlich.*

Beweis. Wir können nach Voraussetzung $L = K(\alpha_1, \ldots, \alpha_n)$ schreiben mit $\alpha_1, \ldots, \alpha_n \in L$. Sei $L_i = K(\alpha_1, \ldots, \alpha_i)$ für $0 \leq i \leq n$. Es ist $L_0 = K$. Dann ist $L_i = L_{i-1}(\alpha_i)$. Da α_i algebraisch über K ist, gilt das auch über L_{i-1}. Also ist $[L_i : L_{i-1}] < \infty$ nach Satz 4.2.13. Der Gradsatz impliziert dann

$$[L : K] = [L_n : L_0] = \prod_{i=1}^{n} [L_i : L_{i-1}] < \infty.$$

□

Satz 4.3.5. *Seien $L \mid M$ und $M \mid K$ algebraische Körpererweiterungen. Dann ist auch die Erweiterung $L \mid K$ algebraisch.*

Beweis. Sei $\alpha \in L$. Nach Voraussetzung ist α algebraisch über M mit Minimalpolynom $\mu_\alpha = X^n + c_1 X^{n-1} + \cdots + c_{n-1} X + c_n \in M[X]$. Da alle Koeffizienten von μ_α in $K(c_1, \ldots, c_n)$ liegen, ist α auch algebraisch über dem Teilkörper $K(c_1, \ldots, c_n)$ von M. Nach Satz 4.2.13 folgt

$$[K(c_1, \ldots, c_n, \alpha) : K(c_1, \ldots, c_n)] < \infty.$$

Da $K(c_1, \ldots, c_n) \mid K$ nach Satz 4.3.4 eine endliche Erweiterung ist, ist nach dem Gradsatz auch $K(c_1, \ldots, c_n, \alpha) \mid K$ eine endliche Erweiterung, also auch eine algebraische Erweiterung. Also ist α algebraisch über K. Das war zu zeigen. □

Korollar 4.3.6. *Seien $L \mid M$ und $M \mid K$ Körpererweiterungen. Dann ist $L \mid K$ genau dann algebraisch, wenn $L \mid M$ und $M \mid K$ algebraisch sind.*

Beweis. Wir müssen nur noch die andere Richtung zeigen, d.h., wenn $L \mid K$ algebraisch ist, so sind es auch $L \mid M$ und $M \mid K$. Das folgt aber direkt aus den Definitionen. □

Beispiel 4.3.7. *Sei $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha$ ist algebraisch über $\mathbb{Q}\}$. Dann ist $\overline{\mathbb{Q}}$ ein Teilkörper von $\mathbb{C}$, da mit $\alpha, \beta \in \overline{\mathbb{Q}}$ auch $\alpha+\beta$ und $\alpha\beta$ in $\overline{\mathbb{Q}}$ liegen, denn $\mathbb{Q}(\alpha, \beta)$ ist eine algebraische Erweiterung über $\mathbb{Q}$ nach Satz* 4.3.4.

Die algebraische Erweiterung $\overline{\mathbb{Q}} \mid \mathbb{Q}$ enthält Zwischenkörper $\mathbb{Q}(\sqrt[n]{p})$ von beliebig hohem Grad $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$, siehe Beispiel 4.2.15. Also gilt

$$[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty.$$

Man sieht also, dass algebraische Erweiterungen nicht endlich sein müssen.

Beispiel 4.3.8. *Die Zahl $\alpha = \sqrt{2} + \sqrt[3]{3}$ ist algebraisch über $\mathbb{Q}$, weil $\sqrt{2}$ und $\sqrt[3]{3}$ algebraisch über $\mathbb{Q}$ sind, mit Minimalpolynomen $X^2 - 2, X^3 - 3 \in \mathbb{Q}[X]$.*

Dieses Argument erspart einem, das Minimalpolynom von $\alpha = \sqrt{2} + \sqrt[3]{3}$ zu suchen. Tatsächlich gilt (Übungsaufgabe)

$$\mu_\alpha = X^6 - 6X^4 - 6X^3 + 12X^2 - 36X + 1.$$

4.4 Automorphismen von Körpererweiterungen

Für einen Körper K bildet die Klasse aller Körpererweiterungen von K zusammen mit den Morphismen von Körperweiterungen über K und der gewöhnlichen Abbildungskomposition eine "Kategorie".

Definition 4.10. Sei $L \mid K$ eine Körpererweiterung. Die *Automorphismengruppe* $\mathrm{Aut}(L \mid K)$ von $L \mid K$ (in der Kategorie der Körpererweiterungen über K) ist durch die Gruppe aller Körperisomorphismen $f \colon L \to L$ gegeben mit $f_{|K} = \mathrm{id}_K$.

Beispiel 4.4.1. *Es gilt* $\mathrm{Aut}(\mathbb{C} \mid \mathbb{R}) \cong C_2$.

Sei $\sigma \in \mathrm{Aut}(\mathbb{C} \mid \mathbb{R})$. Da $\{1, i\}$ eine Basis von $\mathbb{C}$ über $\mathbb{R}$ ist, und $\sigma(1) = 1$ gilt, ist σ durch $\sigma(i)$ schon eindeutig bestimmt. Es gilt

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1,$$

und damit $\sigma(i) = i$ oder $\sigma(i) = -i$. Der erste Fall bedeutet $\sigma = \mathrm{id}$, und der zweite Fall bedeutet, dass σ die komplexe Konjugation ist, d.h., $\sigma(a + bi) = a - bi$. Somit ist $\mathrm{Aut}(\mathbb{C} \mid \mathbb{R}) = \{\mathrm{id}, \sigma\}$.

Beispiel 4.4.2. *Es gilt* $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}) = 1$.

Sei $\sigma \in \mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q})$. Dann ist σ eindeutig bestimmt durch $\sigma(\sqrt[3]{2})$. Es gilt

$$\sigma(\sqrt[3]{2})^3 = \sigma(2) = 2.$$

Da das Polynom $X^2 - 2$ nur die reelle Nullstelle $\sqrt[3]{2}$ hat, folgt $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$ und deshalb $\sigma = \mathrm{id}$.

Im allgemeinen gibt es in algebraischen Körpererweiterungen mehrere Elemente, die das gleiche Minimalpolynom haben. Diese Elemente heißen *konjugiert*. Sie sind der Schlüssel zum Verständnis von Morphismen von Körpererweiterungen der zugehörigen Zwischenkörper. Der Begriff *konjugiert* passt besonders gut auf das folgende Beispiel, nämlich die Erweiterung $\mathbb{C} \mid \mathbb{R}$. Sei $\alpha = i$ und $\beta = -i$. Dann haben beide Elemente das Minimalpolynom $X^2 + 1$ über $\mathbb{R}$. Sie sind also konjugiert.

Satz 4.4.3 (Konjugatiosprinzip)**.** *Seien $L \mid K$ und $L' \mid K'$ Körpererweiterungen, $\sigma\colon K \to K'$ ein Körperisomorphismus und sei $\alpha \in L$ algebraisch über K. Sei $\mu_\alpha \in K[X]$ das Minimalpolynom von α über K. Mit $\mu_\alpha^\sigma \in K'[X]$ bezeichnen wir das Polynom, das man aus μ_α durch Anwendung von σ auf die Koeffizienten erhält.*

(1) *Ist $\widetilde{\sigma}\colon L \to L'$ ein Körpermorphismus mit $\widetilde{\sigma}|_K = \sigma$, so ist $\widetilde{\sigma}(\alpha)$ eine Nullstelle von μ_α^σ in L' und $\widetilde{\sigma}|_{K(\alpha)}$ ist durch $\widetilde{\sigma}(\alpha)$ eindeutig bestimmt.*

(2) *Ist $\beta \in L'$ eine Nullstelle von μ_α^σ, so gibt es genau einen Körperisomorphismus $\widetilde{\sigma}\colon K(\alpha) \to K'(\beta)$ mit $\widetilde{\sigma}|_K = \sigma$ und $\widetilde{\sigma}(\alpha) = \beta$.*

Beweis. Zu (1): Wegen $\mu_\alpha \in K[X]$ und $\widetilde{\sigma}|_K = \sigma$ gilt

$$\mu_\alpha^\sigma(\widetilde{\sigma}(\alpha)) = \widetilde{\sigma}(\mu_\alpha(\alpha)) = \widetilde{\sigma}(0) = 0.$$

Wegen $K(\alpha) = \mathrm{im}(E_\alpha)$, siehe Satz 4.2.13, ist $\widetilde{\sigma}|_{K(\alpha)}\colon K(\alpha) \to L'$ eindeutig bestimmt.

Zu (2): Seien

$$E_\alpha\colon K[X] \to L,$$
$$E_\beta\colon K'[X] \to L'$$

die Einsetzungshomomorphismen zu $\alpha \in L$ bzw. zu $\beta \in L'$. Da μ_α normiert und in $K[X]$ irreduzibel ist und $\sigma\colon K \to K'$ ein Körperisomorphismus ist, ist auch μ_α^σ normiert und in $K'[X]$ irreduzibel. Somit ist μ_α^σ das Minimalpolynom von β. Daher induzieren die Einsetzungshomomorphismen nach Satz 4.2.13 Körperisomorphismen F_α und F_β,

$$\begin{array}{ccc} K[X]/(\mu_\alpha) & \xrightarrow{F_\alpha} & K(\alpha) \\ {\scriptstyle\rho}\downarrow & & \downarrow{\scriptstyle\widetilde{\sigma}} \\ K'[X]/(\mu_\alpha^\sigma) & \xrightarrow[F_\beta]{} & K'(\beta) \end{array}$$

Definieren wir $\rho(f) = f^\sigma$ wie für μ_α, also $\rho(f) = \sum_i \sigma(a_i)X^i$ für $f = \sum_i a_i X^i$, so können wir

$$\widetilde{\sigma} \colon = F_\beta \circ \rho \circ F_\alpha^{-1}$$

definieren. Es ist klar, dass $\widetilde{\sigma}$ ein Körperisomorphismus mit $\widetilde{\sigma}|_K = \sigma$ und $\sigma(\alpha) = F_\beta([X]) = \beta$ ist. Die Eindeutigkeit von $\widetilde{\sigma}$ folgt aus dem ersten Teil. □

Insbesondere können wir Automorphismengruppen von Körpererweiterungen auch als Untergruppen von Symmetriegruppen von Nullstellenmengen auffassen.

Korollar 4.4.4 (Galoisoperation auf den Nullstellen)**.** *Sei $L \mid K$ eine Körpererweiterung und $\alpha \in L$ algebraisch über K. Sei $S \subset K(\alpha)$ die Menge der Nullstellen des Minimalpolynoms μ_α von α in $K(\alpha)$ selbst. Dann gelten folgende Aussagen.*

(1) *Es gilt $K(\beta) = K(\alpha)$ für alle $\beta \in S$.*

(2) *Die Abbildung*

$$\begin{aligned} \mathrm{Aut}(K(\alpha) \mid K) &\to \mathrm{Sym}(S), \\ \sigma &\mapsto (x \mapsto \sigma(x)) \end{aligned}$$

ist ein injektiver Gruppenhomomorphismus. Die zugehörige Gruppenoperation von $\mathrm{Aut}(K(\alpha) \mid K)$ auf S ist transitiv.

(3) *Es gilt*

$$|\mathrm{Aut}(K(\alpha) \mid K)| = |S| \leq [K(\alpha) : K] = \deg(\mu_\alpha).$$

Beweis. Zu (1): Sei $\beta \in S$. Wegen $S \subset K(\alpha)$ folgt $K(\beta) \subset K(\alpha)$. Da α und β konjugiert sind, also das gleiche Minimalpolynom über K besitzen, folgt mit Satz 4.2.13,

$$\begin{aligned} \dim_K(K(\beta)) &= [K(\beta) : K] = \deg(\mu_\beta), \\ \dim_K(K(\alpha)) &= [K(\alpha) : K] = \deg(\mu_\alpha). \end{aligned}$$

Da beide Grade gleich sind, folgt $\dim_K(K(\beta)) = \dim_K(K(\alpha))$. Da diese Vektorraumdimensionen endlich sind, folgt daraus wegen $K(\beta) \subset K(\alpha)$ auch $K(\beta) = K(\alpha)$.

Zu (2): Wegen (1) ist das nur eine Umformulierung des Konjugationsprinzips mithilfe von Gruppenoperationen, für den Fall $\sigma = \mathrm{id}_K \colon K \to K$ mit $K' = K$.

Zu (3): Aus dem Konjugationsprinzip erhalten wir $|\mathrm{Aut}(K(\alpha) \mid K)| = |S|$. Da μ_α in $K(\alpha)$ höchstens $\deg(\mu_\alpha)$ Nullstellen besitzt, folgt die Behauptung zusammen mit Satz 4.2.13. □

Bemerkung 4.4.5. Man beachte, dass es um die Nullstellen von μ_α in $K(\alpha)$ geht, und nicht in einem anderen Körper. Für $\mathbb{C} \mid \mathbb{Q}$ und $\alpha = \sqrt[4]{2}$ ist $\mu_\alpha = X^4 - 2$ und $S = \{\pm\sqrt[4]{2}\}$, obwohl μ_α in $\mathbb{C}$ auch noch die Nullstellen $\pm i\sqrt[4]{2}$ hat.

4.5 Zerfällungskörper

Bei der Untersuchung polynomialer Gleichungen $f(X) = 0$ mit $f \in K[X]$ ist die Frage, in welchem Körper $L \supset K$ man die Lösungen betrachten will. Dabei interessiert man sich insbesondere für den kleinsten Körper, der schon alle denkbaren Nullstellen von f enthält. Für $X^2 + 1 \in \mathbb{Q}[X]$, zum Beispiel, liegen alle Nullstellen in $L = \mathbb{C}$, aber auch schon in $L = \mathbb{Q}(i)$. Das Polynom zerfällt über $\mathbb{Q}(i)$ in Linearfaktoren, d.h., $X^2 + 1 = (X - i)(X + i)$.

Definition 4.11. Sei K ein Körper und $f \in K[X]$ ein Polynom vom Grad $m \geq 1$. In einer Körpererweiterung $L \mid K$ heißt L *Zerfällungskörper von f über K*, falls es Elemente $\alpha_1, \ldots, \alpha_m \in L$ und ein $c \in K$ gibt mit

$$f = c \prod_{i=1}^{m} (X - \alpha_i),$$
$$L = K(\alpha_1, \ldots, \alpha_m).$$

Mit anderen Worten, f zerfällt über L in Linearfaktoren und L wird von den Nullstellen von f erzeugt.

Die Körpererweiterung $L \mid K$ ist also *algebraisch*, da die α_i als Nullstellen von f alle algebraisch über K sind. Da sie endlich erzeugt ist, ist sie auch endlich, siehe Satz 4.3.4.

Beispiel 4.5.1. *1. $\mathbb{C}$ ist ein Zerfällungskörper von $X^2 + 1 \in \mathbb{R}[X]$ über $\mathbb{R}$.*

2. $\mathbb{R}$ ist kein Zerfällungskörper von $X^2 - 2 \in \mathbb{Q}[X]$ über $\mathbb{Q}$.

3. $\mathbb{Q}$ ist ein Zerfällungskörper von $X^2 - 4 \in \mathbb{Q}[X]$ über $\mathbb{Q}$.

In der Tat, bei 2. liegen zwar die Nullstellen $\pm\sqrt{2}$ von $X^2 - 2$ in $\mathbb{R}$, aber $\mathbb{R}$ ist zu groß. Wegen $\pm\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ und $X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ ist $\mathbb{Q}(\sqrt{2})$ der Zerfällungskörper von $X^2 - 2$ über $\mathbb{Q}$.

Beispiel 4.5.2. *Der Zerfällungskörper L von $X^3 - 2 \in \mathbb{Q}[X]$ über $\mathbb{Q}$ ist $\mathbb{Q}(\sqrt[3]{2}, \omega)$, wobei ω eine nicht-triviale dritte Einheitswurzel in $\mathbb{C}$ ist. Es gilt $[L : \mathbb{Q}] = 6$ und $\mathrm{Aut}(L \mid \mathbb{Q}) \cong S_3$.*

Über $\mathbb{C}$ hat $X^3 - 2$ die drei Nullstellen $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$. Es gilt $1 + \omega + \omega^2 = 0$. Nur eine der Nullstellen ist reell, also kann $\mathbb{Q}(\sqrt[3]{2})$ nicht der Zerfällungskörper sein. Sei $\alpha = \sqrt[3]{2}$. Dann ist $\alpha, \omega\alpha, \omega^2\alpha \in L$. Wegen $\omega = \omega\alpha \cdot \frac{1}{\alpha}$ gilt $\mathbb{Q}(\alpha, \omega) \subset L$. Wegen $\omega\alpha, \omega^2\alpha \in \mathbb{Q}(\alpha, \omega)$ gilt auch $L \subset \mathbb{Q}(\alpha, \omega)$. Also hat man $L = \mathbb{Q}(\alpha, \omega)$.

Um $[L : \mathbb{Q}]$ zu bestimmen, erinnern wir zunächst daran, dass $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ gilt, siehe Beispiel 4.2.14. Da $X^2 + X + 1 \in \mathbb{Q}[X]$ das Minimalpolynom von ω über $\mathbb{Q}$ ist, gilt $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$. Nun ist L das Kompositum von $\mathbb{Q}(\alpha)$ und $\mathbb{Q}(\omega)$ in $\mathbb{C} \mid \mathbb{Q}$, und $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ und $[\mathbb{Q}(\omega) : \mathbb{Q}]$ sind teilerfremd. Also können wir Satz 4.2.10 anwenden und erhalten

$$\begin{aligned}[L : \mathbb{Q}] &= [\mathbb{Q}(\alpha)\mathbb{Q}(\omega) : \mathbb{Q}] \\ &= [\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot [\mathbb{Q}(\omega) : \mathbb{Q}] \\ &= 3 \cdot 2 = 6.\end{aligned}$$

Außerdem sehen wir, dass $X^3 - 2$ auch das Minimalpolynom von α über $\mathbb{Q}(\omega)$ ist, weil nach dem Gradsatz gilt

$$\begin{aligned} 6 &= [L : \mathbb{Q}] \\ &= [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\omega)] \cdot [\mathbb{Q}(\omega) : \mathbb{Q}] \\ &= 2 \cdot [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\omega)]. \end{aligned}$$

Die Gruppe $\mathrm{Aut}(L \mid K)$ wird später für spezielle Erweiterungen (nämlich *Galoiserweiterungen*) auch *Galoisgruppe* genannt, und mit $\mathrm{Gal}(L, K)$ bezeichnet. In der Tat ist $\mathbb{Q}(\alpha, \omega) \mid \mathbb{Q}$ eine Galoiserweiterung. Wir wissen aus Korollar 4.4.4, dass $\mathrm{Gal}(L, K)$ eine Untergruppe von $\mathrm{Sym}(S) \cong S_3$ sein muss. Zur Bestimmung dieser Gruppe gehen wir folgt vor:

(1) Wir zeigen, dass die Abbildung

$$\begin{aligned} \mathrm{Gal}(L, \mathbb{Q}) &\to \mathrm{Gal}(\mathbb{Q}(\omega), \mathbb{Q}), \\ \sigma &\mapsto \sigma|_{\mathbb{Q}(\omega)} \end{aligned}$$

einen wohldefinierten Gruppenhomomorphismus liefert.

(2) Wir bestimmen die Gruppe $\mathrm{Gal}(\mathbb{Q}(\omega), \mathbb{Q})$ mit dem Konjugationsprinzip.

(3) Wir bestimmen für jedes Element von $\mathrm{Gal}(\mathbb{Q}(\omega), \mathbb{Q})$ alle möglichen Fortsetzungen zu Elementen von $\mathrm{Gal}(L, \mathbb{Q})$ mit dem Konjugationsprinzip. Damit erhalten wir $\mathrm{Gal}(L, \mathbb{Q})$ als Menge.

(4) Wir bestimmen die Gruppenstruktur auf $\mathrm{Gal}(L, \mathbb{Q})$ durch Berechnung der Werte der Automorphismen auf ω und α und ihren Verknüpfungen.

Zu (1): Sei $\sigma \in \mathrm{Gal}(L, \mathbb{Q})$. Die komplexen Nullstellen von $X^2 + X + 1$ sind $N = \{\omega, \omega^2\}$. Wegen Satz 4.4.3 gilt $\sigma(N) = N$. Also ist

$$\sigma(\mathbb{Q}(\omega)) \subset \mathbb{Q}(\omega).$$

Indem wir das Argument auf σ^{-1} anwenden, sehen wir, dass

$$\sigma|_{\mathbb{Q}(\omega)} \in \mathrm{Gal}(\mathbb{Q}(\omega), \mathbb{Q})$$

gilt.

Zu (2): Wegen $\omega\overline{\omega} = |\omega|^2 = 1^2 = 1$ ist $\omega^2 = \omega^{-1} = \overline{\omega}$ durch komplexe Konjugation gegeben. Wie in Beispiel 4.4.1 erhalten wir, mit Korollar 4.4.4,

$$\mathrm{Gal}(\mathbb{Q}(\omega), \mathbb{Q}) = \{\mathrm{id}, \rho\},$$

wobei ρ die Einschränkung der komplexen Konjugation auf $\mathbb{Q}(\omega)$ bezeichnet.

Zu (3): Wie wir oben gesehen haben, ist $X^3 - 2$ das Minimalpolynom von α über $\mathbb{Q}(\omega)$ und L ist ein Zerfällungskörper von $X^3 - 2$ über $\mathbb{Q}(\omega)$. Daher können wir die Fortsetzungen von $\mathrm{id} = \mathrm{id}|_{\mathbb{Q}(\omega)}$ und ρ auf $\mathrm{Gal}(L, \mathbb{Q})$ mit dem Konjugationsprinzip bestimmen. Die Fortsetzungen von id sind die eindeutig bestimmten Automorphismen, die ω auf ω abbilden, und α wie folgt abbilden:

$$\begin{aligned} \mathrm{id}\colon L \to L,\ \alpha \mapsto \alpha,\\ \sigma\colon L \to L,\ \alpha \mapsto \omega\alpha,\\ \sigma'\colon L \to L,\ \alpha \mapsto \omega^2\alpha. \end{aligned}$$

Die Fortsetzungen von ρ sind die eindeutig bestimmten Automorphismen, die ω auf ω^2 abbilden, und α wie folgt abbilden:

$$\begin{aligned} \tau_1\colon L \to L,\ \alpha \mapsto \alpha,\\ \tau_2\colon L \to L,\ \alpha \mapsto \omega\alpha,\\ \tau_3\colon L \to L,\ \alpha \mapsto \omega^2\alpha. \end{aligned}$$

Dabei folgt aus der Eindeutigkeit, dass $\tau = \tau_2$ mit der komplexen Konjugation auf L übereinstimmt. Also ist

$$\mathrm{Gal}(L, \mathbb{Q}) = \{\mathrm{id}, \sigma, \sigma', \tau_1, \tau, \tau_3\}.$$

Zu (4): Da Elemente aus $\mathrm{Gal}(L, \mathbb{Q})$ eindeutig durch ihre Werte auf α und ω bestimmt sind, können wir die folgenden Beziehungen ablesen:

$$\mathrm{ord}(\sigma) = 3,\ \mathrm{ord}(\tau) = 2,\ \tau\sigma\tau = \sigma^{-1}.$$

In der Tat, es gilt etwa

$$\begin{aligned} \tau^2(\alpha) = \tau(\tau(\alpha)) = \tau(\omega\alpha) = \tau(\omega)\tau(\alpha) = \omega^2\omega\alpha = \alpha,\\ \tau^2(\omega) = \tau(\tau(\omega)) = \tau(\omega^2) = \tau(\omega)\tau(\omega) = \omega^2\omega^2 = \omega. \end{aligned}$$

Also ist $\tau^2 = \mathrm{id}$. Wegen $\tau \neq \mathrm{id}$ folgt $\mathrm{ord}(\tau) = 2$. Mit diesen Relationen gilt $\mathrm{Gal}(L, \mathbb{Q}) = D_3 \cong S_3$, siehe Beispiel 2.1.3.

Bemerkung 4.5.3. Man beachte, dass das Verfahren zur Bestimmung der Galoisgruppe im vorigen Beispiel mit der Zerlegung in $L \mid \mathbb{Q}(\alpha)$ und $\mathbb{Q}(\alpha) \mid \mathbb{Q}$ nicht auf dieselbe Weise funktioniert hätte, da $\mathbb{Q}(\alpha)$ kein Zerfällungskörper von $X^3 - 2$ über $\mathbb{Q}$ ist und sich somit nicht jedes Element von $\mathrm{Gal}(L, \mathbb{Q})$ zu einem Element von $\mathrm{Gal}(\mathbb{Q}(\alpha), \mathbb{Q})$ einschränkt.

Wir kommen nun zur Existenz von Zerfällungskörpern.

Lemma 4.5.4. *Sei $f \in K[X]$ ein nicht-konstantes Polynom. Dann gibt es eine Körpererweiterung $L \mid K$, so dass f über L in Linearfaktoren zerfällt.*

Beweis. Für $\deg(f) = 1$ hat $L = K$ die gewünschte Eigenschaft. Sei also $\deg(f) = n \geq 2$. Wir beweisen das Resultat mit Induktion über n. Ist f reduzibel, so gibt es nicht-konstante Polynome $g, h \in K[X]$ mit $f = gh$ und $\deg(g), \deg(h) < \deg(f)$. Nach

Induktionsvoraussetzung gibt es dann Körpererweiterungen $M \mid K$ und $N \mid M$, so dass g in M und h in N in Linearfaktoren zerfällt. Dann zerfällt auch f in N in Linearfaktoren. Sei also f irreduzibel in $K[X]$. Dann ist $M = K[X]/(f)$ ein Körper, der K enthält. Das Polynom hat in M nach Konstruktion eine Nullstelle, nämlich die Restklasse $[X]$ im Restklassenring M. Damit ist f reduzibel in $M[X]$, und wir können das obige Argument auf $f \in M[X]$ anwenden. □

Satz 4.5.5 (Existenz von Zerfällungskörpern)**.** *Sei $f \in K[X]$ ein nicht-konstantes Polynom über einem Körper K. Dann gibt es einen Zerfällungskörper von f über K.*

Beweis. Sei $L \mid K$ eine Körpererweiterung, so dass f über L in Linearfaktoren zerfällt, siehe Lemma 4.5.4. Dann ist $f = c\prod_{i=1}^{m}(X - \alpha_i)$ mit $\alpha_i \in L$ und $K(\alpha_1, \ldots, \alpha_m)$ ist ein Zerfällungskörper von f über K. □

Zerfällungskörper sind bis auf Isomorphie als Körpererweiterung eindeutig.

Satz 4.5.6. *Sei $\sigma\colon K \to K'$ ein Körperisomorphismus, sei $f \in K[X]$ ein nicht-konstantes Polynom und sei L ein Zerfällungskörper von f über K und L' ein Zerfällungskörper von f^σ über K'. Dann gibt es einen Körperisomorphismus $\widetilde{\sigma}\colon L \to L'$ mit $\widetilde{\sigma}|_K = \sigma$.*

Beweis. Wir führen den Beweis mit Induktion über $\deg(f) = n$. Für $n = 1$ ist $L = K$ und $L' = K'$ und $\widetilde{\sigma} = \sigma$ ist der gesuchte Isomorphismus. Nun setzte man das Resultat für alle Polynome vom Grad kleiner als n voraus. Ist $f \in K[X]$ mit $\deg(f) = n$, so unterscheiden wir zwei Fälle.

Fall 1: Sei f reduzibel über K. Dann gibt es nicht-konstante Polynome $g, h \in K[X]$ mit $f = gh$ und $\deg(g), \deg(h) < n$. Da L ein Zerfällungskörper von f über K ist, gibt es insbesondere ein $m \geq 1$, $c \in K$ und $\alpha_1, \ldots, \alpha_m \in L$ mit

$$g = c \cdot \prod_{j=1}^{m}(X - \alpha_j).$$

Dann ist der Zwischenkörper $M := K(\alpha_1, \ldots, \alpha_m)$ ein Zerfällungskörper von g über K. Analog finden wir einen Zwischenkörper M' von $L' \mid K'$, der ein Zerfällungskörper von g^σ über K ist. Nach Induktionsvoraussetzung gibt es daher einen Körperisomorphismus $\tau\colon M \to M'$ mit $\tau|_K = \sigma$. Wegen $f = gh$ und $f^\sigma = g^\sigma h^\sigma$ sind L bzw. L' Zerfällungskörper von h über M bzw. von h^σ über M'. Nach Induktionsvoraussetzung gibt es somit einen Körperisomorphismus $\widetilde{\sigma}\colon L \to L'$ mit $\sigma|_M = \tau$. Insbesondere ist $\widetilde{\sigma}|_K = \tau|_K = \sigma$. Also sind wir fertig in diesem Fall.

Fall 2: Sei f irreduzibel über K und $\alpha \in L$ eine Nullstelle von f. Dann gibt es ein $g \in K(\alpha)[X]$ mit $f = (X - \alpha)g$. Ebenso sei $\beta \in L'$ eine Nullstelle von f^σ. Da f irreduzibel ist, erhalten wir mit dem Konjugationsprinzip einen Körperisomorphismus $\tau\colon K(\alpha) \to K'(\beta)$ mit $\tau(\alpha) = \beta$ und $\tau|_K = \sigma$. Außerdem ist L ein Zerfällungskörper von g über $K(\alpha)$ und L' ein Zerfällungskörper von g^τ über $K'(\beta)$, denn $f^\sigma = f^\tau = (X-\beta)g^\tau$. Nach Induktionsvoraussetzung gibt es daher einen Körperisomorphismus $\widetilde{\sigma}\colon L \to L'$ mit $\widetilde{\sigma}|_{K(\alpha)} = \tau$. Insbesondere ist $\widetilde{\sigma}|_K = \tau|_K = \sigma$. □

Korollar 4.5.7 (Eindeutigkeit von Zerfällungskörpern). *Sei K ein Körper und $f \in K[X]$ ein nicht-konstantes Polynom. Sind L und M Zerfällungskörper von f über K, so sind die Körpererweiterungen $L \mid K$ und $M \mid K$ isomorph.*

Wir können mithilfe eines Zerfällungskörpers Polynomen $f \in K[X]$ ihre *Galoisgruppe* wie folgt zuordnen.

Definition 4.12 (Galoisgruppe einer Gleichung). Sei K ein Körper und $f \in K[X]$ ein nicht-konstantes Polynom. Ist L ein Zerfällungskörper von f über K, so bezeichnet man $\mathrm{Gal}(L, K)$ auch als *Galoisgruppe von f über K* bzw. als Galoisgruppe der Gleichung $f(X) = 0$ in der Variablen X über K.

Bei der Auflösbarkeit von polynomialen Gleichungen durch iteriertes Wurzelziehen werden die Auflösbarkeitseigenschaften der zugehörigen Galoisgruppen eine entscheidende Rolle spielen.

4.6 Algebraischer Abschluss

Ein Zerfällungskörper eines gegebenen Polynoms $f \in K[X]$ liefert eine endliche algebraische Erweiterung $L \mid K$, in der das Polynom in Linearfaktoren zerfällt. Man kann aber auch eine algebraische Erweiterung finden, in der *alle* nicht-konstanten Polynome $f \in K[X]$ in Linearfaktoren zerfallen. Eine solche Erweiterung ist im allgemeinen nicht endlich.

Definition 4.13 (Algebraischer Abschluss). Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom $f \in K[X]$ mindestens eine Nullstelle in K besitzt. Ein *algebraischer Abschluss* von K ist eine algebraische Körpererweiterung $L \mid K$, wobei L algebraisch abgeschlossen ist.

Beispiel 4.6.1. *1. Der Körper $\mathbb{C}$ ist nach dem Fundamentalsatz der Algebra, siehe* 4.12.2*, algebraisch abgeschlossen. Die Erweiterung $\mathbb{C} \mid \mathbb{R}$ ist somit ein algebraischer Abschluss von $\mathbb{R}$, weil sie eine algebraische Erweiterung ist.*

2. Der Körper $\mathbb{Q}$ ist nicht algebraisch abgeschlossen. Die Erweiterung $\mathbb{C} \mid \mathbb{Q}$ ist kein algebraischer Abschluss von $\mathbb{Q}$, weil die Erweiterung nicht algebraisch ist (die Zahl e ist zum Beispiel nicht algebraisch über $\mathbb{Q}$).

3. Die Erweiterung $\overline{\mathbb{Q}} \mid \mathbb{Q}$ ist ein algebraischer Abschluss von $\mathbb{Q}$, siehe Beispiel 4.3.7*. Sie hat unendlichen Grad.*

4. Ein endlicher Körper ist nicht algebraisch abgeschlossen. Betrachte dazu das nichtkonstante Polynom

$$f = 1 + \prod_{\alpha \in K} (X - \alpha) \in K[X].$$

Es hat keine Nullstelle über K.

Bemerkung 4.6.2. Ein Körper K ist genau dann algebraisch abgeschlossen, wenn jedes nicht-konstante Polynom in $K[X]$ über K in Linearfaktoren zerfällt. Das kann man induktiv mit Theorem 3.10.4 beweisen.

Lemma 4.6.3. *Sei K ein Körper. Dann existiert eine algebraische Körpererweiterung $C(K) \mid K$, so dass jedes nicht-konstante Polynom in $K[X]$ mindestens eine Nullstelle in $C(K)$ besitzt.*

Beweis. Der Beweis ähnelt dem Beweis von Lemma 4.5.4. Für eine Familie von Variablen $(X_i)_{i\in I}$ kann man den zugehörigen Polynomring $K[(X_i)_{i\in I}]$ über K als Vereinigung von Polynomringen in endlich vielen Variablen konstruieren, d.h.,

$$K[(X_i)_{i\in I}] = \bigcup_{J\in\mathcal{F}(I)} K[(X_i)_{i\in J}],$$

wobei $\mathcal{F}(I)$ die Menge aller endlichen Teilmengen von I ist. Für

$$I := K[X] \setminus K$$

sei $R := K[(X_f)_{f\in I}]$ der Polynomring über K mit den Variablen X_f indiziert durch nicht-konstante Polynome f in I. Sei $\mathfrak{a}$ das Ideal in R, das von allen $f(X_f)$ mit $f \in I$ erzeugt wird, also

$$\mathfrak{a} := \operatorname{span}_R\{f(X_f) \mid f \in I\} \subset R.$$

Angenommen es gilt $\mathfrak{a} = R$. Dann gäbe es eine endliche Teilmenge $F \subset I$ und Koeffizienten $(g_f)_{f\in F}$ in R mit

$$1 = \sum_{f\in F} g_f \cdot f(X_f).$$

Mit Satz 4.5.5 erhalten wir einen Erweiterungskörper M von K, in dem jedes $f \in F$ eine Nullstelle $\alpha_f \in M$ besitzt. Nun betrachte man die Abbildung $R \to M$ mit $X_f \mapsto \alpha_f$ für $f \in F$, die alle anderen Variablen auf Null abbildet. Wegen $f(\alpha_f) = 0$ hieße das $1 = 0$ in der obigen Gleichung, ein Widerspruch. Also gilt $\mathfrak{a} \neq R$. Wegen Korollar 3.6.6 gibt es ein maximales Ideal $\mathfrak{m}$ von R mit $\mathfrak{a} \subset \mathfrak{m}$. Der Quotient

$$C(K) := R/\mathfrak{m}$$

ist dann ein Körper, nach Satz 3.6.2, und wir erhalten eine natürliche Einbettung $K \to C(K)$. Nach Konstruktion ist für jedes $f \in K[X]\setminus K$ die Restklasse von X_f in $C(K)$ eine Nullstelle von f. Insbesondere ist die Erweiterung $C(K) \mid K$ algebraisch nach Korollar 4.3.6. □

Korollar 4.6.4 (Existenz eines algebraischen Abschlusses)**.** *Sei K ein Körper. Dann gibt es einen algebraischen Abschluss von K.*

Beweis. Wenden wir die Konstruktion von Lemma 4.6.3 iterativ an, so erhalten wir einen Körperturm

$$K = C^0(K) \subset C^1(K) \subset C^2(K) \subset C^3(K) \subset \cdots$$

Wir betrachten dann die Vereinigung (ein direkter Limes $\varinjlim_n C^n(K)$)

$$L := \bigcup_{n\in\mathbb{N}} C^n(K),$$

welche ein Körper ist, und die zugehörige Körpererweiterung $L \mid K$. Diese ist algebraisch, denn für gegebenes $\alpha \in L$ gibt es ein $n \in \mathbb{N}$ mit $\alpha \in C^n(K)$. Da die Erweiterungen $C^j(K) \mid C^{j-1}(K)$ für alle $0 \leq j \leq n$ algebraisch sind, ist auch $C^n(K) \mid K$ algebraisch nach Korollar 4.3.6. Also ist α algebraisch über K.

Sei $f \in L[X]$ ein Polynom von Grad $\deg(f) \geq 1$. Jeder der endlich vielen nicht-trivialen Koeffizienten von f liegt in einem der Zwischenkörper $C^j(K)$. Indem wir das Maximum der auftretenden Stufen betrachten, erhalten wir ein $n \in \mathbb{N}$ mit $f \in C^n(K)$. Dann besitzt f eine Nullstelle in $C^{n+1}(K)$. Wegen $C^{n+1}(K) \subset L$ hat f also insbesondere eine Nullstelle in L. Damit ist $L \mid K$ ein algebraischer Abschluss von K. □

Beispiel 4.6.5. *Der Körper $\mathbb{F}_p$ besitzt einen algebraischen Abschluss.*

Satz 4.6.6 (Eindeutigkeit algebraischer Abschlüsse)**.** *Sei K ein Körper und sei $M \mid K$ ein algebraischer Abschluss von K. Dann gilt:*

(1) *Ist $L \mid K$ eine algebraische Erweiterung, so gibt es einen Morphismus von $L \mid K$ nach $M \mid K$.*

(2) *Jeder Körpermorphismus $\sigma\colon M \to M$ mit $\sigma|_K = \mathrm{id}_K$ ist ein Isomorphismus.*

(3) *Ist $N \mid K$ ein weiterer algebraischer Abschluss von K, so sind die Erweiterungen $M \mid K$ und $N \mid K$ über K isomorph.*

Beweis. Zu (1): Sei $\mathcal{F}$ die Menge aller Paare (Z, f), wobei Z ein Zwischenkörper der Erweiterung $L \mid K$ ist und $f\colon Z \to M$ ein Körpermorphismus mit $f|_K = \mathrm{id}_K$ ist. Diese Menge ist durch Inklusion und Fortsetzung partiell geordnet und nicht-leer, denn $(K, K \hookrightarrow M) \in \mathcal{F}$. Außerdem besitzt jede total geordnete Kette $(Z_i, f_i)_{i\in I}$ in $\mathcal{F}$ eine obere Schranke in $\mathcal{F}$, nämlich

$$\bigcup_{i\in I} Z_i \to M,\ x \mapsto f_i(x).$$

Nach dem Lemma von Zorn gibt es somit ein maximales Element (Z, f) in $\mathcal{F}$. Wir wollen $Z = L$ zeigen. Dann ist $f\colon L \to M$ der gesuchte Morphismus. Angenommen $Z \neq L$. Dann gibt es ein $\alpha \in L \setminus Z$. Da $L \mid K$ algebraisch ist, ist α algebraisch über K und Z. Sei $\mu_\alpha \in Z[X]$ das Minimalpolynom von α über Z. Da M algebraisch abgeschlossen ist, besitzt μ_α^f eine Nullstelle $\beta \in M$. Nach dem Konjugationsprinzip gibt es somit einen Körpermorphismus

$$\sigma\colon Z(\alpha) \to M$$

mit $\sigma(\alpha) = \beta$ und $\sigma|_Z = f$. Dann ist $(Z(\alpha), \sigma)$ in $\mathcal{F}$ und echt größer als (Z, f), im Widerspruch zur Maximalität von (Z, f).

Zu (2): Wegen Satz 4.1.2 ist σ als Körpermorphismus injektiv. Sei $\beta \in M$. Da $M \mid K$ algebraisch ist, ist β algebraisch über K. Sei $\mu_\beta \in K[X]$ das Minimalpolynom von β. Da σ ein injektiver Körpermorphismus ist, induziert σ nach dem Konjugationsprinzip eine injektive Abbildung von $N \to N$ mit $N = \{x \in M \mid \mu_\beta(x) = 0\}$. Da die Menge dieser Nullstellen endlich ist, ist diese Abbildung bijektiv. Insbesondere liegt β im Bild dieser Abbildung, und damit auch im Bild der Abbildung σ, welche damit auch surjektiv ist. Also ist σ ein Isomorphismus.

Zu (3): Dies folgt aus den ersten beiden Aussagen. Mit dem ersten Teil erhalten wir Körpermorphismen $f\colon M \to N$ und $g\colon N \to M$ mit $f|_K = g|_K = \mathrm{id}_K$. Nach dem zweiten Teil sind $gf\colon M \to M$ und $fg\colon N \to N$ Isomorphismen. Also sind auch f und g bereits Isomorphismen. □

4.7 Endliche Körper

Ein endlicher Körper $\mathbb{F}$ mit Primkörper $P \cong \mathbb{F}_p$ ist als P-Vektorraum isomorph zu P^n, mit $n = \dim_P(\mathbb{F})$. Also gilt $|\mathbb{F}| = p^n$. Somit wissen wir schon einmal, dass es keinen endlichen Körper mit m Elementen geben kann, wenn m keine Primzahlpotentz ist, also zum Beispiel $m = 6$.

Definition 4.14. Sei K ein Körper und sei $f \in K[X]$. Eine Nullstelle $\alpha \in K$ von f ist eine mehrfache Nullstelle von f, wenn $(X - \alpha)^2$ ein Teiler von f in $K[X]$ ist.

Definition 4.15. Die Abbildung $D\colon K[X] \to K[X]$ mit

$$\sum_{j=0}^{n} a_j X^j \mapsto \sum_{j=1}^{n} j a_j X^{j-1}$$

heißt *formale Ableitung* von Polynomen über K.

Satz 4.7.1 (Ableitungskriterium für mehrfache Nullstellen)**.** *Sei K ein Körper und $f \in K[X]$ ein nicht-konstantes, normiertes Polynom. Sei $L \mid K$ eine Körpererweiterung, für die f in $L[X]$ in Linearfaktoren zerfällt. Dann besitzt f genau dann eine mehrfache Nullstelle in L, wenn $\gcd(f, D(f)) \neq 1$ gilt in $K[X]$. Ist f in $K[X]$ irreduzibel, so besitzt f genau dann eine mehrfache Nullstelle in L, wenn $D(f) = 0$ gilt.*

Beweis. Die formale Ableitung ist linear und erfüllt die Leibnizregel, d.h.,

$$\begin{aligned} D(\alpha f + \beta g) &= \alpha D(f) + \beta D(g), \\ D(fg) &= fD(g) + D(f)g \end{aligned}$$

für alle $f, g \in K[X]$ und $\alpha, \beta \in K$. Die erste Eigenschaft rechnet man leicht nach, die zweite muss man wegen der Linearität nur auf Monomen $f = X^i$ und $g = X^j$ überprüfen. Dann ergibt sich

$$D(fg) = (i + j)X^{i+j-1} = jX^iX^{j-1} + iX^{i-1}X^j = fD(g) + D(f)g.$$

Aus der Leibnizregel folgt induktiv

$$D(f^n) = nf^{n-1}D(f)$$

für alle $n \geq 1$. Sei nun α eine mehrfache Nullstelle von f in L und setze $g = X - \alpha$. Dann gilt $g^2 \mid f$. Wir können also $f = g^2 h$ schreiben mit einem $h \in L[X]$. Aus der Leibnizregel folgt

$$D(f) = D(g^2 h) = g(gD(h) + 2D(g)h),$$

also $g \mid gcd(f, D(f))$. Somit ist $\gcd(f, D(f)) \neq 1$ in $L[X]$. Angenommen, $\gcd(f, D(f)) = 1$ in $K[X]$, so hätte man $1 = \gcd(f, D(f)) = \alpha f + \beta D(f)$ in $K[X]$. Diese Gleichung gälte dann auch in $L[X]$, d.h., der ggT wäre auch 1 in $L[X]$, ein Widerspruch. Also ist $\gcd(f, D(f)) \neq 1$ in $K[X]$.

Nehmen wir umgekehrt an, dass f und $D(f)$ einen nicht-trivialen gemeinsamen Faktor in $K[X]$ haben. Dann haben sie einen gemeinsamen linearen Faktor $X - \alpha$ in L. Also ist $f = (X - \alpha)g$ mit einem $g \in L[X]$ und

$$X - \alpha \mid D(f) = D((X - \alpha)g) = (X - \alpha)D(g) + g.$$

Also gilt $X - \alpha \mid g$, so dass $(X - \alpha)^2 \mid f$ gilt in $L[X]$.

Sei nun $f \in K[X]$ irreduzibel. Ist $\alpha \in L$ eine mehrfache Nullstelle, so ist $D(f)(\alpha) = 0$ nach dem ersten Teil und $f = \mu_\alpha$ das Minimalpolynom. Da $\deg(D(f)) < \deg(f)$ gilt, muss schon $D(f) = 0$ sein. Ist umgekehrt $D(f) = 0$, so ist f ein ggT von f und $D(f)$. Also gilt $\gcd(f, D(f)) \neq 1$, und die Behauptung folgt aus dem ersten Teil. □

Theorem 4.7.2. *Sei p eine Primzahl und $k \geq 1$. Dann gibt es bis auf Isomorphie genau einen Körper $\mathbb{F}$ mit p^k Elementen. Ist $P \cong \mathbb{F}_p$ sein Primkörper, so ist $\mathbb{F}$ der Zerfällungskörper des Polynoms $X^{p^k} - X$ über P.*

Beweis. Wir zeigen zuerst die *Eindeutigkeit*. Sei die Existenz eines endlichen Körpers $\mathbb{F}$ mit p^k Elementen bereits gegeben. Dann ist $char(\mathbb{F}) = p$ und wir dürfen $P = \mathbb{F}_p$ annehmen, also die Gleichheit. Sei $f = X^{p^k} - X \in P[X]$. Mit dem Satz von Euler folgt

$$\alpha^{p^k - 1} = 1$$

für alle $\alpha \in \mathbb{F}^\times$, wegen $|(\mathbb{F}^\times, \cdot)| = p^k - 1$. Also gilt $f(\alpha) = \alpha^{p^k} - \alpha = \alpha(\alpha^{p^k - 1} - 1) = 0$ für alle $\alpha \in \mathbb{F}$. Also hat f in $\mathbb{F}$ bereits $p^k = \deg(f)$ Nullstellen und es zerfällt in Linearfaktoren über $\mathbb{F}$. Da jedes Element von $\mathbb{F}$ eine Nullstelle von f ist, wird $\mathbb{F}$ über $\mathbb{F}_p$ von den Nullstellen von f erzeugt. Somit ist $\mathbb{F}$ ein Zerfällungskörper von f über $\mathbb{F}_p$ und damit bis auf Isomorphie eindeutig.

Um die Existenz eines endlichen Körpers $\mathbb{F}$ mit p^k Elementen zu zeigen, definieren wir $\mathbb{F}$ als Zerfällungskörper von f. Wir müssen dann zeigen, dass $|\mathbb{F}| = p^k$ gilt. Sei $N \subset \mathbb{F}$ die Menge der Nullstellen von f in $\mathbb{F}$. Es ist leicht zu sehen, dass N ein Körper ist. Sind

α, β Nullstellen von f, so gilt mit Lemma 4.1.5

$$\begin{aligned}(\alpha+\beta)^{p^k} - (\alpha+\beta) &= \alpha^{p^k} + \beta^{p^k} - (\alpha+\beta)\\ &= 0,\\ (\alpha\beta)^{p^k} - \alpha\beta &= \alpha^{p^k}\beta^{p^k} - \alpha\beta\\ &= (\alpha^{p^k} - \alpha)\beta^{p^k} + \alpha(\beta^{p^k} - \beta)\\ &= 0.\end{aligned}$$

Also sind mit mit $\alpha, \beta \in N$ auch $\alpha+\beta, \alpha\beta \in N$. Zudem sind $0, 1 \in N$ und mit $\alpha \in N$ auch $\alpha^{-1} \in N$. Es ist $(-\alpha)^{p^k} - (-\alpha) = (-1)^{p^k}\alpha^{p^k} - (-\alpha)$, also auch $-\alpha \in N$ für $p > 2$. Für $p = 2$ ist ohnehin $-\alpha = \alpha$. Da N ein Zwischenkörper von $\mathbb{F} \mid \mathbb{F}_p$ ist, der alle Nullstellen von f enthält, folgt somit $N = \mathbb{F}$, also auch $|\mathbb{F}| = |N| \leq \deg(f) = p^k$. Andererseits gilt auch $|N| \geq p^k$, weil f keine mehrfachen Nullstellen hat. In der Tat, $D(f) = p^k X^{p^k-1} - 1 = -1 \neq 0$, und wir folgern die Behauptung aus Satz 4.7.1. □

Wir bezeichnen den bis auf Isomorphie eindeutigen Körper mit p^k Elementen mit $\mathbb{F}_q$, $q = p^k$. Für $k > 1$ ist er als Ring *nicht* isomorph zu $\mathbb{Z}/q\mathbb{Z}$, denn $\mathbb{Z}/q\mathbb{Z}$ hat Nullteiler für $k > 1$ und ist deshalb kein Körper. Das kleinste solche Beispiel eines Körpers ist $\mathbb{F}_4$.

Beispiel 4.7.3. *Es gibt bis auf Isomorphie genau einen Körper mit* 4 *Elementen. Er ist isomorph zu* $\mathbb{F}_2[X]/(X^2+X+1)$ *(Übungsaufgabe).*

Als Ring ist $\mathbb{F}_4$ wie gesagt nicht isomorph zu $\mathbb{Z}/4\mathbb{Z}$, und auch nicht isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ als Ring. Die additive Gruppe $(\mathbb{F}_4, +)$ ist allerdings isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ als Gruppe. In der Tat,

$$(\mathbb{F}_{p^k}, +) \cong (\mathbb{Z}/p\mathbb{Z})^k,$$

da $\mathbb{F}_{p^k}$ ein $\mathbb{F}_p$-Vektorraum der Dimension k ist, also isomorph zu $\mathbb{F}_p^k$ sein muss.

Theorem 4.7.4. *Sei* $\mathbb{F}$ *ein Körper mit* p^k *Elementen. Dann ist die Galoisgruppe* $\mathrm{Gal}(\mathbb{F}, \mathbb{F}_p) \cong C_k$ *zyklisch mit Erzeuger* $\varphi_p \colon \mathbb{F} \to \mathbb{F}$, $\alpha \mapsto \alpha^p$, *dem Frobeniusautomorphismus.*

Beweis. Sei $K = \mathbb{F}_p$ und $\sigma = \varphi_p$. Da σ ein Körperisomorphismus mit $\sigma|_K = \mathrm{id}_K$ ist, gilt $\sigma \in \mathrm{Gal}(\mathbb{F}, K)$. Da $\mathbb{F}^\times$ wegen Korollar 4.1.4 zyklisch ist, gibt es einen Erzeuger $\alpha \in \mathbb{F}^\times$. Man hat $K(\alpha) = \mathbb{F}$ und α ist algebraisch über K, da die Erweiterung $\mathbb{F} \mid K$ endlich ist, nämlich vom Grad $[\mathbb{F} : K] = k$. Also ist, nach Korollar 4.4.4, (3),

$$|\mathrm{Gal}(\mathbb{F}, K)| \leq [\mathbb{F} : K] = k.$$

Es genügt nun, $\mathrm{ord}(\sigma) \geq k$ zu zeigen. Dann ist σ ein Erzeuger der Gruppe $\mathrm{Gal}(\mathbb{F}, K)$, und in der Ungleichung oben gilt die Gleichheit. Sei $\mathrm{ord}(\sigma) = m$. Dann ist $\sigma^m = \mathrm{id}\,|_{\mathbb{F}}$, also $\alpha^{p^m} = \sigma^m(\alpha) = \alpha$. Also sind alle Elemente von $\mathbb{F}$ Nullstellen des Polynoms $X^{p^m} - X \in K[X]$ und somit

$$p^k = |\mathbb{F}| \leq \deg(X^{p^m} - X) = p^m,$$

d.h., $k \leq m$. □

Sei $\overline{\mathbb{F}_p}$ ein algebraischer Abschluss von $\mathbb{F}_p$. Für alle $n \geq 1$ können wir $\mathbb{F}_{p^n}$ nach $\overline{\mathbb{F}_p}$ einbetten. Das Bild dieser Einbettung ist eindeutig bestimmt, wir bezeichnen es ebenfalls mit $\mathbb{F}_{p^n}$.

Korollar 4.7.5. *Es gilt*

$$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n$$

und die Erweiterungen $\mathbb{F}_{p^m} \mid \mathbb{F}_{p^n}$ für $m \mid n$ sind bis auf Isomorphie die einzigen Erweiterungen endlicher Körper der Charakteristik $p > 0$.

Beweis. Wir wissen, dass $\mathbb{F}_{p^k}$ die Menge der $\alpha \in \overline{\mathbb{F}_p}$ mit $\alpha^{p^k} = \alpha$ ist. Sei $\alpha \in \mathbb{F}_{p^m}$. Es gilt $\alpha^{p^{dm}} = \alpha^{p^m} = \alpha$. Sei $m \mid n$, also $n = md$. Dann folgt $\alpha^{p^n} = \alpha$, also $\alpha \in \mathbb{F}_{p^n}$, d.h., $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$.

Ist umgekehrt $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$, so ist $\mathbb{F}_{p^n}$ ein Vektorraum über $\mathbb{F}_{p^m}$ der Dimension, sagen wir, d. Dann gilt $|\mathbb{F}_{p^n}| = |\mathbb{F}_{p^m}|^d$, also

$$p^n = (p^m)^d = p^{md},$$

also $m \mid n$. Die zweite Aussage überlassen wir dem Leser. □

4.8 Galoiserweiterungen

Definition 4.16. Eine algebraische Körpererweiterung $L \mid K$ heißt *normal*, wenn für jedes $\alpha \in L$ das Minimalpolynom $\mu_\alpha \in K[X]$ von α über K in L in Linearfaktoren zerfällt.

Die Benennung hat mit dem Normalteilerbegriff von Gruppen zu tun, der in der Korrespondenz von Körpererweiterungen und Galoisgruppen auftritt. Wie wir schon in Beispiel 4.5.2 gesehen haben, ist die Erweiterung $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ nicht normal, denn $X^3 - 2$ zerfällt in $\mathbb{Q}(\sqrt[3]{2})$ nicht in Linearfaktoren. Es gilt $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}) = 1$, siehe Beispiel 4.4.2, aber $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

Beispiel 4.8.1. *1. Jede Körpererweiterung vom Grad 2 ist normal.*

2. Ist $L \mid K$ ein algebraischer Abschluss eines Körpers K, so ist die Körpererweiterung $L \mid K$ normal.

3. Die Körpererweiterungen $L \mid M$ und $M \mid K$ mit $L = \mathbb{Q}(\sqrt[4]{2})$, $M = \mathbb{Q}(\sqrt{2})$ und $K = \mathbb{Q}$ sind normal, aber die Erweiterung $L \mid K$ ist nicht normal.

Das dritte Beispiel zeigt, dass Normalität von Körpererweiterungen im allgemeinen nicht transitiv ist, wie auch in der Gruppentheorie. Die ersten beiden Erweiterungen haben Grad 2, sind also normal. Die letzte kann nicht normal sein, da $X^4 - 2$ nicht alle Nullstellen in L hat.

Die folgenden beiden Kriterien helfen in vielen Fällen, Normalität nachzuweisen.

Satz 4.8.2. *Sei $L \mid K$ eine algebraische Körpererweiterung und sei $M \mid L$ ein algebraischer Abschluss von L. Dann sind äquivalent:*

(1) *Die Körpererweiterung $L \mid K$ ist normal.*

(2) *Es gibt eine Teilmenge $S \subset L$ mit $L = K(S)$ und der Eigenschaft, dass für jedes $\alpha \in S$ das Minimalpolynom von α über K in $L[X]$ in Linearfaktoren zerfällt.*

(3) *Für jeden Körpermorphismus $\sigma\colon L \to M$ mit $\sigma|_K = \mathrm{id}_K$ gilt bereits $\sigma(L) \subset L$.*

Beweis. (1) $\Longrightarrow$ (2): Das folgt direkt mit $S = L$.

(2) $\Longrightarrow$ (3): Das folgt aus dem Konjugationsprinzip. Sei S eine Menge wie in Aussage (2) und $\sigma\colon L \to M$ ein Körpermorphismus mit $\sigma|_K = \mathrm{id}_K$. Wegen $L = K(S)$ genügt es zu zeigen, dass $\sigma(S) \subset L$ ist. Aus der Voraussetzung, dass das Minimalpolynom von α über K bereits über L in Linearfaktoren zerfällt, folgt mit dem Konjugationsprinzip, Satz 4.4.3, dass $\sigma(\alpha) \subset L$.

(3) $\Longrightarrow$ (1): Angenommen, (3) gilt. Sei $\alpha \in L$ und μ_α das Minimalpolynom von α über K. Da μ_α über dem algebraischen Abschluss M in Linearfaktoren zerfällt, genügt es zu zeigen, dass alle M-Nullstellen von μ_α bereits in L liegen. Dann ist $L \mid K$ normal. Sei also $\beta \in M$ eine Nullstelle von μ_α. Nach dem Konjugationsprinzip existiert dann ein Körpermorphismus $\sigma\colon K(\alpha) \to M$ mit $\sigma|_K = \mathrm{id}_K$ und $\sigma(\alpha) = \beta$. Analog zum Beweis von Satz 4.6.6 zur Eindeutigkeit algebraischer Abschlüsse können wir mithilfe des Konjugationsprinzips und des Zornschen Lemmas den Körpermorphismus σ zu einem Körpermorphismus $\widetilde{\sigma}\colon L \to M$ mit $\widetilde{\sigma}|_{K(\alpha)} = \sigma$ fortsetzen. Nach Voraussetzung ist dann

$$\beta = \sigma(\alpha) = \widetilde{\sigma}(\alpha) \in \widetilde{\sigma}(L) \subset L.$$

□

Beispiel 4.8.3. *1. Sei L ein Zerfällungskörper von $f \in K[X]$ über K. Dann ist die Erweiterung $L \mid K$ normal.*

2. Jede algebraische Erweiterung $L \mid K$ eines endlichen Körpers K ist normal.

Für die erste Aussage sei $\sigma\colon L \to \overline{L}$ ein Körpermorphismus mit $\sigma|_K = \mathrm{id}_K$. Er bildet die Nullstellen von f in sich ab. Da L ein Zerfällungskörper von f über K ist, wird L von diesen Nullstellen erzeugt, d.h., es gilt $\sigma(L) = L$. Also ist (3) von Satz 4.8.2 erfüllt und $L \mid K$ deshalb normal.

Für die zweite Aussage sei $\alpha \in L$ und $M := K(\alpha)$. Dann ist $M \mid K$ eine endliche Erweiterung. Also ist M ein Zerfällungskörper eines Polynoms über dem Primkörper P von K nach Theorem 4.7.2. Somit ist $M \mid P$ nach dem ersten Teil normal. Dann ist nach Definition auch $M \mid K$ normal.

Wir formulieren den letzten Punkt nochmals als Satz.

Satz 4.8.4. *Sei $L \mid K$ eine normale Erweiterung. Dann ist für jeden Zwischenkörper M in $L \mid K$ die Erweiterung $L \mid M$ normal.*

Beweis. Sei $\alpha \in L$. Sei $\mu_{\alpha,K}$ das Minimalpolynom von α über K. Sei $\mu_{\alpha,M}$ das Minimalpolynom von α über M. Dann gilt $\mu_{\alpha,M} \mid \mu_{\alpha,K}$ in $M[X]$. Zerfällt also $\mu_{\alpha,K}$ in Linearfaktoren über K, dann gilt das auch für $\mu_{\alpha,M}$. □

Definition 4.17. Sei K ein Körper und $M \mid K$ ein algebraischer Abschluss von K. Ein Polynom $f \in K[X]$ ungleich 0 heißt *separabel* über K, wenn es über M in paarweise verschiedene Linearfaktoren zerfällt, also keine mehrfachen Nullstellen in M besitzt.

Beispiel 4.8.5. *1. Das Polynom $X^3 - 2 \in \mathbb{Q}[X]$ ist separabel über $\mathbb{Q}$.*

2. Das Polynom $X^3 - 2 \in \mathbb{F}_3[X]$ ist inseparabel über $\mathbb{F}_3$.

3. Ein Polynom $f \in K[X]$ ungleich 0 ist genau dann separabel, wenn es relativ prim zu $D(f)$ in $K[X]$ ist.

In der Tat, $X^3-2 = (X+1)^3$ hat mehrfache Nullstellen über $\mathbb{F}_3$. Der dritte Punkt folgt aus dem Ableitungskriterium, Satz 4.7.1. Die Aussage kann für irreduzible Polynome noch verbessert werden.

Satz 4.8.6. *Sei K ein Körper und $f \in K[X]$ ein irreduzibles Polynom. Dann ist f genau dann separabel über K wenn $D(f) \neq 0$ gilt. Hat K Charakteristik Null, dann ist jedes irreduzible Polynom $f \in K[X]$ separabel. In Charakteristik p ist ein irreduzibles Polynom $f \in K[X]$ genau dann separabel, wenn es* kein *Polynom in X^p ist.*

Beweis. Die erste Behauptung haben wir schon in Satz 4.7.1 gezeigt. Es gilt $D(f) \neq 0$ für Charakeritsik Null, da jedes nicht-konstante Polynom nicht-verschwindende Ableitung hat. Also sind alle irreduziblen Polynome in $K[X]$ separabel. In Charakteristik p gilt folgendes. Sei $f \in K[X]$ ein irreduzibles inseparables Polynom, dann ist $D(f) = 0$. Schreiben wir $f = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$, so bedeutet $D(f) = 0$, dass $ic_i = 0$ in K für $0 \leq i \leq n$, mit $c_n = 1$. Das bedeutet $p \mid i$ für alle i mit $c_i \neq 0$. Also sind nur die Koeffizienten von f nicht Null, die in durch p teilbaren Graden auftreten. Insbesondere ist $n = \deg(f)$ ein Vielfachens von p, etwa $n = pm$. Schreiben wir jeden Exponenten eines nicht-verschwindenden Terms in f als ein Vielfaches von p, so erhalten wir

$$\begin{aligned} f &= X^{pm} + c_{p(m-1)}X^{p(m-1)} + \cdots + c_pX^p + c_0 \\ &= g(X^p) \end{aligned}$$

für ein $g \in K[X]$. Also ist $f \in K[X^p]$.

Ist umgekehrt $f(X) = g(X^p)$ ein Polynom in X^p, dann gilt

$$D(f)(X) = D(g)(X^p)pX^{p-1} = 0.$$

Also ist f inseparabel, falls es irreduzibel ist. □

Beispiel 4.8.7. *Sei p eine Primzahl und $K = \mathbb{F}_p(Y)$. Dann ist das Polynom $X^p - Y \in K[X]$ irreduzibel nach Eisenstein, denn Y ist ein Primelement in K, und inseparabel nach Satz* 4.8.6. *Insbesondere ist die Körpererweiterung $K[X]/(X^p-Y) \mid K$ algebraisch, aber nicht separabel.*

Definition 4.18. Sei $L \mid K$ eine Körpererweiterung. Ein über K algebraisches Element $\alpha \in L$ heißt *separabel* über K, wenn das Minimalpolynom von α über K separabel ist. Eine algebraische Körpererweiterung $L \mid K$ heißt *separabel*, wenn jedes $\alpha \in L$ separabel über K ist.

Definition 4.19. Sei $L \mid K$ eine Körpererweiterung und $M \mid K$ ein algebraischer Abschluss von K. Dann bezeichnet $[L : K]_s$ die Anzahl der Körpermorphismen $\sigma\colon L \to M$ mit $\sigma|_K = \mathrm{id}_K$, den sogenannten *Separabilitätsgrad* der Erweiterung $L \mid K$. Für die Menge dieser Körpermorphismen schreiben wir auch $\mathrm{Hom}_K(L, M)$.

Bemerkung 4.8.8. Die obigen Begriffe sind unabhängig vom gewählten algebraischen Abschluss, da algebraische Abschlüsse bis auf Isomorphie eindeutig bestimmt sind und die obigen Eigenschaften unter Isomorphie von Körpererweiterungen erhalten bleiben.

Satz 4.8.9. *Jede algebraische Erweiterung $L \mid K$ eines endlichen Körpers K ist normal und separabel.*

Beweis. Die Normalität hatten wir in Beispiel 4.8.3 gezeigt. Sei $\mathrm{char}(K) = p$ und $\alpha \in L \setminus 0$. Das Minimalpolynom μ_α von α über K ist ein Teiler des Polynoms $X^{p^k} - X$, siehe den Beweis von Satz 4.7.2. Da $f = X^{p^k} - X$ mit $D(f) = p^k X^{p^k - 1} - 1 = -1$ nach dem Ableitungskriterium über K separabel ist, ist somit auch μ_α über K separabel. Also ist die Körperweiterung $L \mid K$ separabel. □

Bemerkung 4.8.10. Ein Körper K heißt *perfekt*, wenn jede algebraische Erweiterung über K separabel ist. Somit sind also endliche Körper perfekt, und alle Körper der Charakteristik Null, wegen Satz 4.8.6. Hingegen ist $\mathbb{F}_p(Y)$ nicht perfekt nach Beispiel 4.8.7.

Satz 4.8.11 (Separabilität von einfachen Erweiterungen)**.** *Sei $L \mid K$ eine Körpererweiterung und sei $\alpha \in L$ algebraisch über K. Dann ist α genau dann separabel über K wenn $[K(\alpha) : K]_s = [K(\alpha) : K]$ gilt.*

Beweis. Sei $n = \deg(\mu_\alpha)$. Ist α separabel über K, so hat f keine mehrfachen Nullstellen, sondern n paarweise verschiedene. Nun ist $[K(\alpha) : K]_s$ gleich der Anzahl der verschiedene Nullstellen von f in einem algebraischen Abschluss von K, nach dem Konjugatiosprinzip. Also ist

$$[K(\alpha) : K]_s = n = \deg(\mu_\alpha) = [K(\alpha) : K].$$

Gilt umgekehrt diese Gleichheit, so hat μ_α genau n verschiedene Nullstellen, also ist α separabel über K. □

Folgender Satz sei noch ohne Beweis erwähnt.

Satz 4.8.12. *Seien $M \mid L \mid K$ algebraische Körpererweiterungen. Dann gilt*

$$[M : K]_s = [M : L]_s \cdot [L : K]_s.$$

Bemerkung 4.8.13. Hat K Charakteristik p, so existiert ein $r \geq 0$ mit $[L : K] = p^r \cdot [L : K]_s$. Insbesondere ist $[L : K]_s$ ein Teiler von $[L : K]$.

Satz 4.8.14. *Sei $L \mid K$ eine endliche separable Erweiterung. Dann gilt $[L : K]_s = [L : K]$.*

Beweis. Nach Voraussetzung ist $L = K(\alpha_1, \ldots, \alpha_n)$ und α_{i+1} ist für alle $i = 1, \ldots, n-1$ separabel über K, also auch über $K(\alpha_1, \ldots, \alpha_i)$. Aus Satz 4.8.11 folgt

$$[K(\alpha_1, \ldots, \alpha_{i+1}) : K(\alpha_1, \ldots, \alpha_i)]_s = [K(\alpha_1, \ldots, \alpha_{i+1}) : K(\alpha_1, \ldots, \alpha_i)].$$

Wegen des Gradsatzes und des Satzes 4.8.12 folgt die Behauptung. □

Bemerkung 4.8.15. Sei $L \mid K$ eine endliche Erweiterung. Dann gilt auch die Umkehrung des obigen Satzes, d.h., wenn $[L : K]_s = [L : K]$ gilt, so ist $L \mid K$ separabel. Für Charakteristik Null ist das klar. Für Charakteristik p kann man die Bemerkung 4.8.13 verwenden.

Satz 4.8.16. *Seien $M \mid L \mid K$ algebraische Körpererweiterungen. Dann ist $M \mid K$ genau dann separabel, wenn $M \mid L$ und $L \mid K$ separabel sind.*

Beweis. Ist $M \mid K$ separabel, so ist jedes Element von M separabel über K, also auch über L wegen $\mu_{\alpha,L} \mid \mu_{\alpha,K}$ in $L[X]$. Weiterhin ist auch jedes Element von $L \subset M$ separabel über K. Also sind $M \mid L$ und $L \mid K$ separabel.

Seien umgekehrt $M \mid L$ und $L \mid K$ separabel und $\alpha \in M$ gegeben. Es sei E der Zwischenkörper von $L \mid K$, der von den Koeffizienten des Minimalpolynoms $\mu_\alpha \in L[X]$ erzeugt wird. Da $M \mid L$ separabel ist, so ist μ_α separabel. Somit ist $E(\alpha) \mid E$ separabel. Da $L \mid K$ separabel ist, ist auch $E \mid K$ separabel. Ferner sind $E \mid K$ und $E(\alpha) \mid K$ endlich. Also gilt mit Satz 4.8.12, Satz 4.8.14 und dem Gradsatz

$$\begin{aligned}[E(\alpha) : K]_s &= [E(\alpha) : E]_s \cdot [E : K]_s \\ &= [E(\alpha) : E] \cdot [E : K] \\ &= [E(\alpha) : K].\end{aligned}$$

Nach Bemerkung 4.8.15 ist $E(\alpha) \mid K$ separabel, also ist α separabel über K. □

Eine Körpererweiterung $L \mid K$ der Form $L = K(\alpha)$ heißt *einfach*, und α heißt *primitives Element*.

Theorem 4.8.17 (Satz vom primitiven Element)**.** *Sei $L \mid K$ eine endliche separable Körpererweiterung. Dann gibt es ein primitives Element $\alpha \in L$ mit $L = K(\alpha)$. Insbesondere gilt $[L : K]_s = [L : K]$ und jede endliche Erweiterung $L \mid K$ in Charakteristik Null ist einfach.*

Beweis. Wir müssen nur den ersten Teil zeigen, d.h., dass es ein primitives Element gibt. Dann folgt $[L : K]_s = [L : K]$ aus Satz 4.8.11 und jede endliche Erweiterung $L \mid K$ in Charakteristik Null ist *separabel* nach Bemerkung 4.8.10, also einfach nach dem ersten Teil.

Sei K endlich. Dann ist auch L nach Voraussetzung endlich, und somit $(L^\times, \cdot)$ zyklisch

nach Korollar 4.1.4. Insbesondere hat dann jeder Erzeuger α von $L^\times$ die Eigenschaft, dass $L = K(\alpha)$ ist.

Wir dürfen also annehmen, dass K unendlich ist. Es genügt zu zeigen, dass jede endliche Erweiterung $L := K(\beta, \gamma)$ ein primitives Element besitzt und dann induktiv zu argumentieren. Sei $n = [L : K]_s$ und M ein algebraischer Abschluss von K und $\mathrm{Hom}_K(L, M) = \{\sigma_1, \ldots, \sigma_n\}$. Wir betrachten das Polynom

$$f = \prod_{1 \le j < k \le n} ((\sigma_j(\beta) - \sigma_k(\beta)) + (\sigma_j(\gamma) - \sigma_k(\gamma))X)$$

in $M[X]$. Es ist nicht das Nullpolynom, da $\sigma_i \neq \sigma_j$ für $i \neq j$ und diese Automorphismen wegen $L = K(\beta, \gamma)$ durch ihre Werte auf β und γ eindeutig bestimmt sind. Also besitzt f in K nur endlich viele Nullstellen. Da K unendlich ist, gibt es somit ein $x \in K$ mit $f(x) \neq 0$. Wir betrachten nun die Elemente α und $\sigma_j(\alpha)$ mit

$$\begin{aligned} \alpha &= \beta + x\gamma \in L \\ \alpha_j &= \sigma_j(\beta) + x\sigma_j(\gamma) = \sigma_j(\alpha) \end{aligned}$$

Wegen $f(x) \neq 0$ sind die Elemente $\alpha_1, \ldots, \alpha_n$ paarweise verschieden. Sei $\mu_\alpha \in K[X]$ das Minimalpolynom von α über K. Mit dem Konjugationsprinzip folgt dann, dass μ_α in L mindestens die n Nullstellen $\alpha_1, \ldots, \alpha_n$ besitzt. Also ist

$$[K(\alpha) : K] = \deg(\mu_\alpha) \ge n.$$

Es bleibt $K(\alpha) = L$ zu zeigen. Angenommen, es gibt ein $\delta \in L \setminus K(\alpha)$. Dann gilt, wegen 4.8.11 und $[K(\alpha) : K] \ge n$,

$$\begin{aligned} n &= [L : K]_s \\ &\ge [K(\alpha, \delta) : K]_s \\ &= [K(\alpha, \delta) : K(\alpha)]_s \cdot [K(\alpha) : K]_s \\ &= [K(\alpha, \delta) : K(\alpha)]_s \cdot [K(\alpha) : K] \\ &\ge [K(\alpha, \delta) : K(\alpha)]_s \cdot n. \end{aligned}$$

Da $\delta \notin K(\alpha)$ und da das Minimalpolynom von δ über K und dann auch über $K(\alpha)$ nach Voraussetzung separabel ist, folgt mit Satz 4.8.11

$$[K(\alpha, \delta) : K(\alpha)]_s = [K(\alpha, \delta) : K(\alpha)] > 1.$$

Also folgt von oben $n = [L : K]_s > 1 \cdot n$, was nicht sein kann. Also ist doch $K(\alpha) = L$. □

Beispiel 4.8.18. *1. Die Erweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid \mathbb{Q}$ ist einfach, und es gilt*

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

2. Die Erweiterungen $\overline{\mathbb{Q}} \mid \mathbb{Q}$ und $\mathbb{R} \mid \mathbb{Q}$ sind nicht einfach.

Nach Satz 4.3.4 ist jede einfache algebraische Erweiterung endlich. Wäre $\overline{\mathbb{Q}} \mid \mathbb{Q}$ eine einfache Erweiterung, so wäre sie endlich, da sie algebraisch ist. Das ist ein Widerspruch. Da einfache Erweiterungen von $\mathbb{Q}$ abzählbar sind, wäre $\mathbb{R}$ abzählbar, falls $\mathbb{R} \mid \mathbb{Q}$ einfach wäre.

Definition 4.20. Eine *Galoiserweiterung* $L \mid K$ ist eine algebraische Körpererweiterung, die normal und separabel ist. In diesem Fall bezeichnen wir $\mathrm{Gal}(L, K) := \mathrm{Aut}(L \mid K)$ als die *Galoisgruppe* der Erweiterung $L \mid K$.

Bemerkung 4.8.19. Die *Galoistheorie* geht auf den französischen Mathematiker Évariste Galois zurück. Er lebte vom 25. Oktober 1811 bis 31. Mai 1832 und starb bei einem Duell mit nur 20 Jahren. Galois hat die Auflösbarkeit von polynomialen Gleichungen durch Radikale untersucht. Er hat die Galoisgruppe als Symmetriegruppe der Lösungen eingeführt und den Zusammenhang zwischen algebraischen Eigenschaften der Galoisgruppe von Zerfällungskörpern und der Auflösbarkeit von polynomialen Gleichungen entdeckt. Diese Erkenntnisse hat er in in der Nacht vor seinem Duell am 30. Mai 1832 in einem Brief an seinen Freund Auguste Chevalier skizziert.

Beispiel 4.8.20. *1. Jede algebraische Erweiterung $\mathbb{F} \mid \mathbb{F}_q$ eines endlichen Körpers $\mathbb{F}_q$ ist nach Satz* 4.8.9 *eine Galoiserweiterung.*

2. Ist K ein Körper der Charakteristik Null oder ein endlicher Körper, so ist jeder algebraische Abschluss $\overline{K} \mid K$ von K eine Galoiserweiterung (siehe 4.8.1, 4.8.9 *und* 4.8.10*).*

3. Ist K ein Körper der Charakteristik Null und ist $f \in K[X]$ normiert, so liefert jeder Zerfällungskörper L von f über K eine Galoiserweiterung $L \mid K$, siehe Satz 4.8.2*.*

4. Die Erweiterung $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ ist keine Galoiserweiterung, da sie nicht normal ist.

5. Die Erweiterung $\mathbb{F}_p(Y)[X]/(X^p - Y) \mid \mathbb{F}_p(Y)$ ist keine Galoiserweiterung, da sie nicht separabel ist, siehe Beispiel 4.8.7*.*

Satz 4.8.21 (Grad endlicher Galoiserweiterungen)**.** *Sei $L \mid K$ eine endliche Galoiserweiterung. Dann ist*

$$[L : K] = [L : K]_s = |\mathrm{Gal}(L, K)|.$$

Beweis. Nach dem Satz vom primitiven Element gibt es ein $\alpha \in L$ mit $L = K(\alpha)$ und

$$[L : K] = [L : K]_s = [K(\alpha) : K]_s.$$

Da die Körpererweiterung $L \mid K$ normal ist, erhalten wir aus dem Konjugationsprinzip mit Satz 4.4.3 und Satz 4.8.2 auch

$$[K(\alpha) : K]_s = |\mathrm{Gal}(L, K)|.$$

□

Definition 4.21. Sei $L \mid K$ eine Körpererweiterung und G eine Untergruppe von $\mathrm{Aut}(L \mid K)$. Dann ist

$$L^G = \{a \in L \mid \sigma(a) = a \text{ für alle } \sigma \in G\}$$

ein Zwischenkörper von $L \mid K$. Er heißt *Fixkörper* von G.

Satz 4.8.22 (Fixkörper)**.** *Sei $L \mid K$ eine Körpererweiterung und G eine endliche Untergruppe von $\mathrm{Aut}(L \mid K)$. Dann ist $L \mid L^G$ eine Galoiserweiterung mit*

$$[L : L^G] = |G|,$$
$$\mathrm{Gal}(L, L^G) = G.$$

Beweis. Wir zeigen zunächst, dass $L \mid L^G$ separabel ist. Sei $\alpha \in L$. Dann ist für jedes $\sigma \in G$ das Element $\sigma(\alpha) \in L$ eine Nullstelle von μ_{α,L^G}. Somit gibt es endlich viele, paarweise verschiedene $\sigma_1, \ldots, \sigma_m$ mit

$$\mathcal{S} = (\sigma_1(\alpha), \ldots, \sigma_m(\alpha)) = \{\sigma(\alpha) \mid \sigma \in G\}.$$

Jedes $\sigma \in G$ vermittelt eine Abbildung

$$\mathcal{S} \to \mathcal{S},\ \sigma_i(\alpha) \mapsto \sigma \circ \sigma_i(\alpha).$$

Da $\mathrm{id}(\alpha) = \alpha$ ist, ist ferner $\alpha \in \mathcal{S}$. Wir betrachten das Polynom

$$f := \prod_{j=1}^{m} (X - \sigma_j(\alpha)) \in L[X]$$

Für alle $\sigma \in G$ gilt

$$f^\sigma = \prod_{j=1}^{m} (X - \sigma \circ \sigma_j(\alpha)) = f,$$

d.h. alle Koeffizienten von f werden von σ festgehalten. Somit ist bereits $f \in L^G[X]$. Ferner ist f nach Konstruktion ein separables Polynom mit $f(\alpha) = 0$. Damit ist α separabel über L^G, d.h. $L \mid L^G$ ist separabel. Ferner ist $L \mid L^G$ normal, da L Zerfällungskörper aller Polynome f des obigen Typs über L^G ist. Also ist $L \mid L^G$ eine Galoiserweiterung.

Sei S eine endliche Teilmenge von L. Da $L \mid L^G$ separabel ist, ist auch die Erweiterung $L^G(S) \mid L^G$ separabel. Letztere Erweiterung ist endlich wegen Satz 4.2.10 über Grade von Komposita. Also gibt es nach dem Satz vom primitiven Element ein $\alpha \in L$ mit $L^G(S) = L^G(\alpha)$. Nach dem ersten Teil folgt

$$[L^G(S) : L^G] = [L^G(\alpha) : L^G] \leq |G|.$$

Nun ist L die Vereinigung aller Teilkörper $L^G(S)$ mit $L^G(S) \mid L^G$ endlich. Man wähle ein S, so dass der Grad $[L^G(S) : L^G]$ maximal ist. Dann erfüllt jedes $a \in L$

$$[L^G(S)(a) : L^G] \leq [L^G(S) : L^G],$$

also $L^G(S)(a) = L^G(S)$ für alle $a \in L$. Damit ist $L = L^G(S) = L^G(\alpha)$, siehe oben, mit

$$[L : L^G] \leq |G|.$$

Mit Satz 4.8.21 folgt, da $G \leq \mathrm{Gal}(L, L^G)$,

$$|G| \leq |\mathrm{Gal}(L, L^G)| = [L : L^G] \leq |G|.$$

Also gilt die Gleichheit. Da G endlich ist, folgt auch $G = \mathrm{Gal}(L, L^G)$. □

Korollar 4.8.23 (Fixkörper der Galoisgruppe)**.** *Sei $L \mid K$ eine endliche Galoiserweiterung. Dann ist*

$$L^{\mathrm{Gal}(L,K)} = K.$$

Beweis. Sei $G = \mathrm{Gal}(L, K)$. Einerseits ist $[L : K] = |G|$ wegen Satz 4.8.21. Andererseits gilt $[L : L^G] = |G|$ wegen Satz 4.8.22. Mit der Multiplikativität des Grades erhalten wir also

$$[L^G : K] = \frac{[L : K]}{[L : L^G]} = \frac{|G|}{|G|} = 1,$$

und damit $L^G = K$. □

Das Korollar gilt übrigens auch für unendliche Galoiserweiterungen. Wir erhalten noch ein weiteres Korollar aus Satz 4.8.22, nämlich, dass sich jede endliche Gruppe als eine Galoisgruppe einer endlichen Galoiserweiterung realisieren läßt.

Korollar 4.8.24. *Sei G eine endliche Gruppe der Ordnung n. Dann gibt es eine Galoiserweiterung $L \mid K$ mit* $\mathrm{Gal}(L, K) \cong G$.

Beweis. Für einen beliebigen Körper E operiert die Gruppe S_n via Permutation der Variablen durch Körperisomorphismen auf dem Körper $L = E(X_1, \ldots, X_n)$. Dadurch erhält man eine zu S_n isomorphe Untergruppe $S \leq \mathrm{Gal}(L, E)$ und G ist isomorph zu einer Untergruppe $H \leq S$. Nun setzte man $K := L^H$. Nach Satz 4.8.22 ist dann $L \mid K$ eine endliche Galoiserweiterung mit

$$\mathrm{Gal}(L, K) = \mathrm{Gal}(L, L^H) = H \cong G.$$

□

Bemerkung 4.8.25. Dieses Korollar gilt im allgemeinen nicht für unendliche Gruppen. Für unendliche Galoiserweiterungen $L \mid K$ hat man die Krull Topologie als natürliche Topologie, die $\mathrm{Gal}(L, K)$ dann zu einer pro-endlichen Gruppe macht, d.h., zu einer kompakten, total unzusammenhängenden Hausdorff topologischen Gruppe. Allerdings kann man abzählbar unendliche Gruppen nicht zu pro-endlichen Gruppen machen.

Bemerkung 4.8.26. Im Beweis des Korollars haben wir kaum Kontrolle über den Grundkörper K für den Isomorphismus $G \cong \mathrm{Gal}(L, K)$. So kann man also im allgemeinen nicht sagen, ob das Korollar auch für einen vorgeschriebenen Grundkörper gilt.

Es ist in der Tat ein berühmtes offenes Problem, das **Inverse Galois Problem**, welche endliche Gruppen als Galoisgruppe einer Galoiserweiterung über $K = \mathbb{Q}$ auftreten können, und mit welchem Polynom. Das Inverse Galois Problem fragt, ob *jede* endliche Gruppe als eine solche Galoisgruppe über $K = \mathbb{Q}$ auftritt. Für viele Klassen endlicher Gruppen ist eine positive Antwort bekannt, z.B., für alle endlichen abelschen Gruppen (Kronecker-Weber), alle endlichen auflösbaren Gruppen (Shafarevich), alle Gruppen S_n und A_n (Hilbert), und alle sporadischen endlichen einfachen Gruppen bis auf die Mathieu Gruppe M_{23} der Ordnung 10200960. Bei den Serien einfacher Gruppen ist die Frage bereits offen für $PSL(2, 3^3)$ der Ordnung 9828 (Stand 2019).

Wir kommen nun zu einem der der wichtigsten Sätze dieser Vorlesung. Es bezeichne $\mathcal{U}(G)$ die Menge aller Untergruppen einer Gruppe G und $\mathcal{Z}(L \mid K)$ die Menge aller Zwischenkörper einer Erweiterung $L \mid K$.

Theorem 4.8.27 (Der Hauptsatz der Galoistheorie)**.** *Es sei $L \mid K$ eine endliche Galoiserweiterung und $G = \mathrm{Gal}(L, K)$. Dann sind die Abbildungen*

$$\begin{aligned} \mathcal{Z}(L, K) &\to \mathcal{U}(G), \quad M \mapsto \mathrm{Gal}(L, M) \\ \mathcal{U}(G) &\to \mathcal{Z}(L \mid K), \quad H \mapsto L^H \end{aligned}$$

zueinander inverse Bijektionen.
Sei M ein Zwischenkörper von $L \mid K$. Dann ist die Körpererweiterung $M \mid K$ genau dann normal, wenn $\mathrm{Gal}(L, M)$ ein Normalteiler in $\mathrm{Gal}(L, K)$ ist. In diesem Fall ist

$$\begin{aligned} \mathrm{Gal}(L, K)/\mathrm{Gal}(L, M) &\to \mathrm{Gal}(M, K), \\ [\sigma] &\mapsto \sigma|_M \end{aligned}$$

ein Gruppenisomorphismus.

Beweis. Sei $H \leq G$ eine Untergruppe. Da G endlich ist nach Satz 4.8.21, ist auch H endlich. Dann ist L^H ein Zwischenkörper von $L \mid K$ und Satz 4.8.22 liefert $\mathrm{Gal}(L, L^H) = H$. Sei umgekehrt M ein Zwischenkörper von $L \mid K$. Dann ist $L \mid M$ eine endliche Galoiserweiterung und wir wissen nach Korollar 4.8.24, dass $M = L^{Gal(L,M)}$ gilt.

Für die zweite Aussage, sei $M \mid K$ normal. Dann ist die Abbildung

$$\begin{aligned} \pi\colon\ \mathrm{Gal}(L, K) &\to \mathrm{Gal}(M, K), \\ \sigma &\mapsto \sigma|_M \end{aligned}$$

nach dem Konjugationsprinzip ein wohldefinierter Gruppenhomomorphismus mit $\mathrm{im}(\pi) = Gal(M, K)$. Sein Kern ist

$$\ker(\pi) = \{\sigma \in \mathrm{Gal}(L, K) \mid \sigma|_M = \mathrm{id}_M\} = \mathrm{Gal}(L, M).$$

Also ist $\mathrm{Gal}(L, M)$ ein Normalteiler in $\mathrm{Gal}(L, K)$ und die Behauptung folgt aus dem Homomorphiesatz. Sei umgekehrt H ein Normalteiler in $\mathrm{Gal}(L, K)$ und $\alpha \in M$. Wir müssen zeigen, dass $M \mid K$ normal ist. Da $L \mid K$ eine normale Körpererweiterung ist, zerfällt

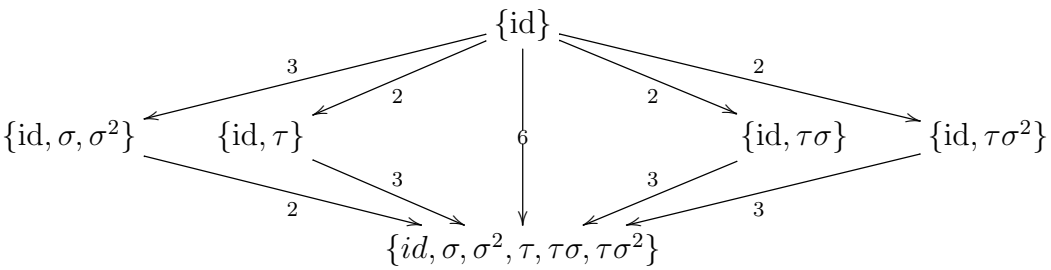
$\mu_{\alpha,K}$ über L in Linearfaktoren und es genügt zu zeigen, dass jede Nullstelle von $\mu_{\alpha,K}$ in L bereits in M liegt. Sei also $\beta \in L$ eine Nullstelle von $\mu_{\alpha,K}$. Durch mehrfache Anwendung des Konjugationsprinzips erhalten wir einen Körperisomorphismus $\sigma \in \mathrm{Gal}(L,K)$ mit $\sigma(\alpha) = \beta$. Da H ein Normalteiler in $\mathrm{Gal}(L,K)$ ist, gilt $H = \sigma H \sigma^{-1}$. Wegen

$$(\sigma \circ \tau \circ \sigma^{-1})(\beta) = (\sigma \circ \tau)(\alpha) = \sigma(\alpha) = \beta$$

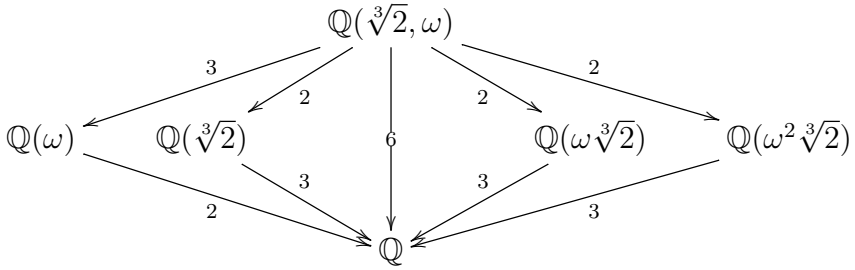
für alle $\tau \in H \leq \mathrm{Gal}(L, L^H)$, gilt $\beta \in L^{\sigma H \sigma^{-1}} = L^H$. Nach dem ersten Teil ist also $\beta \in L^H = M$. □

Bemerkung 4.8.28. Die Bijektionen sind inklusionsumkehrend, d.h., aus $H, H' \in \mathcal{U}(G)$ mit $H \subset H'$ folgt $L^H \supset L^{H'}$, und aus $M, M' \in \mathcal{Z}(L \mid K)$ mit $M \subset M'$ folgt $\mathrm{Gal}(L,M) \supset \mathrm{Gal}(L,M')$.

Beispiel 4.8.29. *Die Erweiterung $\mathbb{Q}(\sqrt[3]{2}, \omega) \mid \mathbb{Q}$ aus Beispiel 4.5.2 ist eine Galoiserweiterung mit Galoisgruppe $G = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega), \mathbb{Q}) \cong S_3$. Die Untergruppen von G,*



entsprechen den Zwischenkörpern von $\mathbb{Q}(\sqrt[3]{2}, \omega) \mid \mathbb{Q}$,



Die Erweiterung $\mathbb{Q}(\sqrt[3]{2}, \omega) \mid \mathbb{Q}$ ist normal, da sie ein Zerfällungskörper des Polynoms $X^3 - 2$ über $\mathbb{Q}$ ist, siehe Satz 4.8.2. Sie ist separabel, da alle algebraischen Erweiterungen in Charakteristik Null separabel sind, siehe Bemerkung 4.8.10. Also ist sie eine Galoiserweiterung. Ihre Galoisgruppe ist $D_3 \cong S_3$, wie wir schon in Beispiel 4.5.2 nachgerechnet haben. Jede echte Untergruppe von S_3 hat Ordnung 2 oder 3 nach Lagrange. Eine Untergruppe der Ordnung 2 ist eine 2-Sylowgruppe. Davon gibt es genau drei Untergruppen. Ebenso gibt es genau eine 3-Sylowgruppe, die isomorph zu $A_3 \cong C_3$ ist. Damit erhalten wir insgesamt 6 Untergruppen, die wir im Diagramm dargestellt mit den Indexzahlen versehen haben. Man kann nun leicht nachrechnen, dass die Unterkörper genau den im Diagramm angegebenen Untergruppen entsprechen. Dabei sind die Untergruppen der Ordnung 2 nicht normal, wie auch die kubischen Zwischenkörper keine normalen Erweiterungen über $\mathbb{Q}$ sind. Natürlich ist A_3 ein Normalteiler von S_3, d.h., $\mathbb{Q}(\omega) \mid \mathbb{Q}$ eine normale Erweiterung.

Satz 4.8.30 (Kompositum)**.** *Sei $L \mid K$ eine endliche Galoiserweiterung mit Zwischenkörpern E und E'. Es seien $H = \mathrm{Gal}(L, E)$ und $H' = \mathrm{Gal}(L, E')$. Dann gelten folgende Aussagen.*

(1) $E \subset E' \iff H' \subset H$.

(2) $EE' = L^{H \cap H'}$.

(3) $E \cap E' = L^{\langle H, H' \rangle}$.

Beweis. Zu (1): Für $E \subset E'$ ist nach Definition

$$H' = \mathrm{Gal}(L, E') \subset \mathrm{Gal}(L, E) = H.$$

Umgekehrt gilt für $H' \subset H$ nach dem Hauptsatz der Galoistheorie

$$E = L^H \subset L^{H'} = E'.$$

Zu (2): Offenbar ist $EE' \subset L^{H \cap H'}$. Umgekehrt folgt aus $E \subset EE'$ und $E' \subset EE'$ mit (1)

$$\mathrm{Gal}(L, EE') \subset \mathrm{Gal}(L, E) \cap \mathrm{Gal}(L, E') = H \cap H'.$$

Daraus folgt, wieder mit (1),

$$L^{H \cap H'} \subset EE'.$$

Zu (3): Offenbar ist $L^{\langle H, H' \rangle} = L^H \cap L^{H'} = E \cap E'$, wobei $\langle H, H' \rangle$ die von H und H' erzeugte Untergruppe von $\mathrm{Gal}(L, K)$ ist. □

Damit kann man folgenden Satz zeigen.

Satz 4.8.31. *Es sei $L \mid K$ eine Körpererweiterung mit Zwischenkörpern E und E', so dass $E \mid K$ und $E' \mid K$ endliche Galoiserweiterungen sind. Dann gilt:*

(1) *Die Erweiterung $EE' \mid K$ ist eine endliche Galoiserweiterung und die Abbildung*

$$\begin{aligned} \mathrm{Gal}(EE', E) &\to \mathrm{Gal}(E', E \cap E'), \\ \sigma &\to \sigma|_{E'} \end{aligned}$$

ist ein Gruppenisomorphismus.

(2) *Die Abbildung*

$$\begin{aligned} \mathrm{Gal}(EE', K) &\to \mathrm{Gal}(E, K) \times \mathrm{Gal}(E', K), \\ \sigma &\to (\sigma|_E, \sigma|_{E'}) \end{aligned}$$

ist ein injektiver Gruppenhomomorphismus, der genau dann ein Isomorphismus ist wenn $E \cap E' = K$ gilt.

4.9 Kreisteilungskörper

Definition 4.22. Sei $n \geq 2$ und ζ_n eine *primitive* n-te Einheitswurzel in $\mathbb{C}$, d.h., eine n-te Einheitswurzel, die keine k-te Einheitswurzel mit $k < n$ ist. Dann heißt der Körper $\mathbb{Q}(\zeta_n)$ der *n-te Kreisteilungskörper* in $\mathbb{C}$. Das Minimalpolynom $\Phi_n \in \mathbb{Q}[X]$ von ζ_n über $\mathbb{Q}$ heißt *n-tes Kreisteilungspolynom.*

Der Name soll an die geometrische Lage der n-ten Einheitswurzeln auf dem Einheitskreis erinnern. Mit $(\mathbb{Z}/n\mathbb{Z})^\times$ bezeichen wir die *prime Restklassengruppe.* Die n-ten Einheitswurzeln in $\mathbb{C}$ bilden eine endliche Gruppe der Ordnung n unter Multiplikation. Sie ist zyklisch, da jede endliche Untergruppe von $\mathbb{C}^\times$ nach Satz 4.1.3 zyklisch ist.

Definition 4.23. Die Menge der primitiven n-ten Einheitswurzeln in $\mathbb{C}$ ist gegeben durch $U_n = \{\zeta_n^k \mid 1 \leq k \leq n,\ \gcd(k,n) = 1\}$. Mit $U(n)$ sei die Gruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ bezeichnet. Es gilt $|U(n)| = |U_n| = \varphi(n)$.

Satz 4.9.1. *Es sei $\zeta_n \in \overline{Q}$ eine primitive n-te Einheitswurzel und $P = \prod_{\zeta \in U_n}(X - \zeta)$. Dann ist $\mathbb{Q}(\zeta_n) \mid \mathbb{Q}$ eine Galoiserweiterung mit $\Phi_n = P$ und $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.*

Beweis. Offenbar ist $X^n - 1$ ein separables Polynom in $\mathbb{Q}[X]$, dessen Nullstellen alle in $\mathbb{Q}(\zeta_n)$ liegen. Als Zerfällungskörper von $X^n - 1$ ist $\mathbb{Q}(\zeta_n) \mid \mathbb{Q}$ eine Galoiserweiterung. Wir zeigen, dass das Minimalpolynom von ζ_n über $\mathbb{Q}$, also Φ_n, mit P übereinstimmt und deshalb den Grad $\varphi(n)$ hat. Da das Minimalpolynom irreduzibel über $\mathbb{Q}$ ist, ist es auch separabel. Es genügt also zu zeigen, dass P und Φ_n die gleichen Nullstellen in $\mathbb{C}$ besitzen. Sei $\alpha \in \mathbb{C}$ eine Nullstelle von Φ_n. Dann gibt es nach dem Konjugationsprinzip ein $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n), \mathbb{Q})$ mit $\sigma(\zeta_n) = \alpha$, also mit

$$\mathrm{ord}(\alpha) = \mathrm{ord}(\sigma(\zeta_n)) = \mathrm{ord}(\zeta_n) = n.$$

Jede Nullstelle von von Φ_n ist also eine primitive n-te Einheitswurzel in U_n, also eine Nullstelle von P.

Sei umgekehrt $\zeta \in \mathbb{C}$ eine Nullstelle von P. Dann gibt es ein $1 \leq k \leq n-1$ mit $\zeta = \zeta_n^k$ und $\gcd(n,k) = 1$. Dann entsteht ζ aus ζ_n durch wiederholtes Potenzieren mit den Primteilern von k. Wir dürfen also induktiv annehmen, dass $k = p$ prim ist, und $p \nmid n$. Da ζ_n eine Nullstelle von $X^n - 1$ ist, gilt $\Phi_n \mid X^n - 1$ und es gibt ein $g \in \mathbb{Q}[X]$ mit $X^n - 1 = g\Phi_n$. Da $X^n - 1 \in \mathbb{Z}[X]$, und Φ_n, g normiert sind, folgt nach dem Lemma von Gauß 3.9.2, dass $g, \Phi_n \in \mathbb{Z}[X]$ gilt. Angenommen, $\Phi_n(\zeta_n^p) \neq 0$. Wegen

$$0 = (\zeta_n^p) - 1 = (g\Phi_n)(\zeta_n^p) = g(\zeta_n^p)\Phi_n(\zeta_n^p)$$

muss dann $g(\zeta_n^p) = 0$ gelten. Also ist ζ_n eine Nullstelle von $g(X^p) \in \mathbb{Z}[X]$ und deshalb $\Phi_n \mid g(X^p)$ in $\mathbb{Q}[X]$. Es gibt also ein $h \in \mathbb{Q}[X]$ mit $g(X^p) = h\Phi_n$. Nach dem Lemma von Gauß folgt wiederum $h \in \mathbb{Z}[X]$. Sei $\pi\colon \mathbb{Z}[X] \to \mathbb{F}_p[X]$ der Reduktionshomomorphismus modulo p. Dann ist

$$\pi(g)^p = \pi(g^p) = \pi(g(X^p)) = \pi(h\Phi_n) = \pi(h)\pi(\Phi_n).$$

Insbesondere haben $\pi(\Phi_n)$ und $\pi(g)$ in $\mathbb{F}_p[X]$ einen gemeinsamen Primteiler. Also ist das Polynom

$$X^n - [1] = \pi(X^n - 1) = \pi(g)\pi(\Phi_n) \in \mathbb{F}_p[X]$$

nicht separabel. Wegen $p \nmid n$ steht dies jedoch im Widerspruch zum Ableitungskriterium, Satz 4.7.1. Also ist doch $\Phi_n(\zeta_n^p) = 0$. □

Satz 4.9.2. *Sei $\mathbb{Q}(\zeta_n)$ der n-te Kreisteilungskörper und $f \in \mathrm{Gal}(\mathbb{Q}(\zeta_n), \mathbb{Q})$ gegeben durch $f(\zeta_n) = \zeta_n^k$ für ein $k \in \mathbb{Z}$. Dann ist die Abbildung*

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\zeta_n), \mathbb{Q}) &\to (\mathbb{Z}/n\mathbb{Z})^\times, \\ f &\to [k] \end{aligned}$$

ein Gruppenisomorphismus.

Beweis. Es ist leicht zu sehen, dass die Abbildung ein injektiver Gruppenhomomorphismus ist. Wegen

$$|\mathrm{Gal}(\mathbb{Q}(\zeta_n), \mathbb{Q})| = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$$

ist er auch surjektiv. □

Beispiel 4.9.3. *Die Kreisteilungspolynome $\Phi_n \in \mathbb{Z}[X]$ für $1 \leq n \leq 10$ sind wie folgt gegeben (siehe auch Beispiel* 3.10.14 *für $n = p$ prim).*

$$\begin{aligned} \Phi_1 &= X - 1 \\ \Phi_2 &= X + 1 \\ \Phi_3 &= X^2 + X + 1 \end{aligned}$$

$$\begin{aligned} \Phi_4 &= X^2 + 1 \\ \Phi_5 &= X^4 + X^3 + X^2 + X + 1 \\ \Phi_6 &= X^2 - X + 1 \\ \Phi_7 &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\ \Phi_8 &= X^4 + 1 \\ \varphi_9 &= X^6 + X^3 + 1 \\ \varphi_{10} &= X^4 - X^3 + X^2 - X + 1 \end{aligned}$$

Hierbei kann man die Polynome rekursiv berechnen durch die Identität

$$X^n - 1 = \prod_{d|n} \Phi_d.$$

Die Identität folgt wegen

$$\begin{aligned} X^n - 1 &= \prod_{1 \leqslant k \leqslant n} \left(X - e^{2i\pi \frac{k}{n}} \right) \\ &= \prod_{d \mid n} \prod_{\substack{1 \leqslant k \leqslant n \\ \gcd(k,n)=d}} \left(X - e^{2i\pi \frac{k}{n}} \right) \\ &= \prod_{d \mid n} \Phi_{\frac{n}{d}} \\ &= \prod_{d \mid n} \Phi_d. \end{aligned}$$

4.10 Auflösbarkeit durch Radikale

Wir beantworten nun die Frage, welche polynomialen Gleichungen durch iteriertes Wurzelziehen gelöst werden können. Der Einfachheit halber beschränken wir uns dabei auf den Fall von *Charakteristik Null*.

Definition 4.24. Eine *Wurzelerweiterung* ist eine Erweiterung $L \mid K$, so dass es ein $\alpha \in L$, ein $n \geq 1$ und ein $c \in K$ mit $L = K(\alpha)$ und $\alpha^n = c$ gibt. Eine Körpererweiterung $L \mid K$ heißt *durch Radikale auflösbar*, falls es eine Erweiterung $M \mid K$ mit $M \supset L \supset K$ gibt, und eine Kette von Zwischenkörpern

$$M_0 = K \subset M_1 \subset \cdots \subset M_n = M$$

gibt, so dass $M_j \mid M_{j-1}$ für jedes $1 \leq j \leq n$ eine Wurzelerweiterung ist.

Ein normiertes Polynom $f \in K[X]$ ist *über K durch Radikale auflösbar*, wenn für einen (dann jeden) Zerfällungskörper L von f über K die zugehörige Erweiterung $L \mid K$ durch Radikale auflösbar ist.

Beispiel 4.10.1. *Seien $b, c \in K$. Dann ist das Polynom $f = X^2 + bX + c \in K[X]$ durch Radikale auflösbar.*

Sei $M \mid K$ ein algebraischer Abschluss von K und sei $\alpha \in M$ eine Wurzel aus $b^2 - 4c$, d.h., mit $\alpha^2 = b^2 - 4c$. Dann ist $K(\alpha) \mid K$ in $M \mid K$ eine Wurzelerweiterung von K und $K(\alpha)$ ist ein Zerfällungskörper von f, denn in $K(\alpha)[X]$ gilt

$$f = \left(X - \frac{-b + \alpha}{2} \right) \left(X - \frac{-b - \alpha}{2} \right).$$

Satz 4.10.2. *Sei $n \in \mathbb{N}$ und K ein Körper, der ein Element $\zeta \in K^\times$ der Ordnung n enthält. Sei $L \mid K$ eine endliche Erweiterung. Dann gilt:*

(1) *Falls es ein $\alpha \in L$ mit $L = K(\alpha)$ und $\alpha^n \in K$ gibt, so ist $L \mid K$ eine zyklische Galoiserweiterung, d.h., eine Galoiserweiterung mit zyklischer Galoisgruppe.*

(2) *Falls $L \mid K$ eine zyklische Galoiserweiterung mit* $\mathrm{Gal}(L,K) \cong \mathbb{Z}/n\mathbb{Z}$ *ist, so ist $L \mid K$ eine Wurzelerweiterung.*

Beweis. Zu (1): Ist $\alpha \in L$ und gilt $L = K(\alpha)$ mit $\alpha^n = c$, so ist $L = K(\alpha)$ ein Zerfällungskörper von $X^n - c$ über K wegen

$$X^n - c = \prod_{k=0}^{n} (X - \zeta^k \alpha).$$

Wegen $\mathrm{ord}(\zeta) = n$ sind alle Nullstellen von $X^n - c$ verschieden, d.h., das Polynom ist separabel über K und α ist separabel über K. Also ist $L \mid K$ nach Satz 4.8.2 und Satz 4.8.11 eine Galoiserweiterung. Mit dem Konjugationsprinzip, Korollar 4.4.4 kann man nun sehen, dass $\mathrm{Gal}(L,K)$ zyklisch ist (Übungsaufgabe).

Zu (2): Sei umgekehrt $L \mid K$ eine Galoiserweiterung und $\sigma \in \mathrm{Gal}(L,K)$ ein Erzeuger mit $\mathrm{ord}(\sigma) = n$. Wir fassen σ als K-linearen Endomorphismus von L auf. Man kann zeigen, dass es eine primitive n-te Einheitswurzel in K gibt, die ein Eigenwert von σ ist. Sei $\alpha \in L$ ein zugehöriger Eigenvektor. Dann liegt $c := \alpha^n$ in K. Wie im ersten Teil sieht man, dass $K(\alpha)$ ein Zerfällungskörper von $X^n - c$ über K ist. Mit einer Gradabschätzung erhalten wir nun, dass $L = K(\alpha)$ ist (Übungsaufgabe). □

Jede endliche Körpererweiterung L von $\mathbb{Q}$ (also ein Zahlkörper) ist isomorph zu einem Unterkörper von $\mathbb{C}$. Wir wollen hier annehmen, dass bereits $L \subset \mathbb{C}$ gilt.

Satz 4.10.3. *Sei $L \mid \mathbb{Q}$ eine endliche Körpererweiterung und sei $\zeta \in \mathbb{C}$ eine Einheitswurzel. Dann gilt:*

(1) *Die Erweiterung $L \mid \mathbb{Q}$ ist genau dann durch Radikale auflösbar, wenn die Erweiterung $L(\zeta) \mid \mathbb{Q}(\zeta)$ durch Radiakle auflösbar ist.*

(2) *Sei $L \mid \mathbb{Q}$ eine Galoiserweiterung. Dann ist die Gruppe* $\mathrm{Gal}(L,\mathbb{Q})$ *genau dann auflösbar, wenn die Gruppe* $\mathrm{Gal}(L(\zeta),\mathbb{Q}(\zeta))$ *auflösbar ist.*

Beweis. Zu (1): Das folgt aus der Tatsache, dass $L(\zeta) \mid L$ und $Q(\zeta) \mid \mathbb{Q}$ Wurzelerweiterungen sind und dass Verschiebungen von Wurzelerweiterungen durch Bildung des Kompositums mit einem gegebenen Körper wieder Wurzelerweiterungen sind.

Zu (2): Es gilt $L(\zeta) = L\mathbb{Q}(\zeta)$. Es ist $\mathbb{Q}(\zeta) \mid \mathbb{Q}$ eine *abelsche* Galoiserweiterung, siehe Satz 4.9.2, also mit abelscher Galoisgruppe. Ebenso sieht man auch, dass $L(\zeta) \mid L$ eine abelsche Galoiserweiterung ist. Mit dem Hauptsatz der Galoistheorie erhalten wir eine Erweiterung

$$1 \to \mathrm{Gal}(L(\zeta),L) \to \mathrm{Gal}(L(\zeta),\mathbb{Q}) \to \mathrm{Gal}(L,\mathbb{Q}) \to 1.$$

Die Gruppe $\mathrm{Gal}(L(\zeta),\mathbb{Q})$ ist genau dann aufösbar, wenn $\mathrm{Gal}(L(\zeta),L)$ und $\mathrm{Gal}(L,\mathbb{Q})$ auflösbar sind, siehe Satz 2.10.6 und Satz 2.10.7. Da $\mathrm{Gal}(L(\zeta),L)$ abelsch und damit auflösbar ist, erhält man, dass $\mathrm{Gal}(L(\zeta),\mathbb{Q})$ genau dann aufösbar ist, wenn $\mathrm{Gal}(L,\mathbb{Q})$ auflösbar ist. Ebenso liefert die Erweiterung

$$1 \to \mathrm{Gal}(L(\zeta),\mathbb{Q}(\zeta)) \to \mathrm{Gal}(L(\zeta),\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta),\mathbb{Q}) \to 1,$$

dass $\mathrm{Gal}(L(\zeta), \mathbb{Q})$ genau dann aufösbar ist, wenn $\mathrm{Gal}(L(\zeta), \mathbb{Q}(\zeta))$ auflösbar ist. Daraus folgt die Behauptung. □

Satz 4.10.4 (Normale Hülle von Wurzelerweiterungen)**.** *Sei $K \mid \mathbb{Q}$ eine endliche normale Körpererweiterung und $n \in \mathbb{N}$. Sei $\alpha \in C$ mit $c = \alpha^n \in K$. Dann gibt es einen Zwischenkörper L von $\mathbb{C} \mid K(\alpha)$, so dass $L \mid K(\alpha)$ durch Radikale auflösbar ist und $L \mid \mathbb{Q}$ normal ist.*

Beweis. Sei $N := \{x \in \mathbb{C} \mid x^n = \sigma(c) \text{ mit } \sigma \in \mathrm{Gal}(K, \mathbb{Q})\}$ und $L := K(N) \subset \mathbb{C}$. Nach Konstruktion ist L ein Zwischenkörper von $\mathbb{C} \mid K(\alpha)$ und die Erweiterung $L \mid K(\alpha)$ ist durch Radikale auflösbar. Da $K \mid \mathbb{Q}$ normal ist, gilt $\sigma(c) \in K$ für alle $\sigma \in \mathrm{Gal}(K, \mathbb{Q})$. Ausserdem ist die Erweiterung $L \mid \mathbb{Q}$ normal, da das Polynom

$$f := \prod_{\sigma \in \mathrm{Gal}(K,\mathbb{Q})} (X^n - \sigma(c)) \in K[X]$$

über L in Linearfaktoren zerfällt, nach Konstruktion von L, und da $\mathbb{C}$ algebraisch abgeschlossen ist. Nach Konstruktion von f gilt $f^\sigma = f$ für alle $\sigma \in \mathrm{Gal}(K, \mathbb{Q})$ und damit $f \in K^{\mathrm{Gal}(K,\mathbb{Q})}[X]$. Nach Korollar 4.8.24 ist $K^{\mathrm{Gal}(K,\mathbb{Q})} = \mathbb{Q}$ und somit $f \in \mathbb{Q}[X]$. Insbesondere sind die Minimalpolynome über $\mathbb{Q}$ der Elemente von N Teiler von f und zerfallen über L in Linearfaktoren. Damit ist $L \mid \mathbb{Q}$ nach Satz 4.8.2 normal. □

Nun kommen wir zu dem Hauptresultat über Auflösbarkeit polynomialer Gleichungen durch Radikale.

Theorem 4.10.5. *Sei $f \in \mathbb{Q}[X]$ ein nicht-konstantes Polynom. Dann ist f genau dann über $\mathbb{Q}$ durch Radikale auflösbar, wenn die Galoisgruppe von f über $\mathbb{Q}$ auflösbar ist.*

Beweis. Sei f über $\mathbb{Q}$ durch Radikale auflösbar und sei L ein Zerfällungskörper von f über $\mathbb{Q}$, den man aus den komplexen Nullstellen von f gewinnen kann. Mithilfe der normalen Hüllen aus Satz 4.10.4 erhalten wir induktiv einen Zwischenkörper M von $\mathbb{C} \mid L$ mit folgenden Eigenschaften:

(1) Die Erweiterung $M \mid \mathbb{Q}$ ist normal.

(2) Die Erweiterung $M \mid \mathbb{Q}$ ist durch Radikale auflösbar, wobei die Wurzeltürme bei M enden.

Sei $n \in \mathbb{N}$ das Produkt der Exponenten in einer Kette von Wurzelerweiterungen von $\mathbb{Q}$ nach M und sei $\zeta := e^{2\pi i/n} \in \mathbb{C}$. Dann ist $L(\zeta) \mid \mathbb{Q}(\zeta)$ eine Galoiserweiterung, die nach Satz 4.10.3 durch Radikale auflösbar ist. Mit dem Fall einer einzelnen Wurzelerweiterung über einem Grundkörper mit passenden Einheitswurzeln (Satz 4.10.2), den Gruppenerweiterungen aus dem Hauptsatz der Galoistheorie folgt induktiv, dass die Gruppe $\mathrm{Gal}(M(\zeta), \mathbb{Q}(\zeta))$ auflösbar ist. Nach Satz 4.10.3 ist dann auch $\mathrm{Gal}(M, \mathbb{Q})$ auflösbar. Da $L \mid \mathbb{Q}$ normal ist, folgt mit einer weiteren Anwendung des Hauptsatzes der Galoistheorie, dass $\mathrm{Gal}(L, \mathbb{Q})$ als Quotient von $\mathrm{Gal}(M, \mathbb{Q})$ ebenfalls auflösbar ist.

Sei umgekehrt $L \mid \mathbb{Q}$ ein Zerfällungskörper von f über $\mathbb{Q}$ mit $L \subset \mathbb{C}$ und sei

$G := \mathrm{Gal}(L, \mathbb{Q})$ auflösbar und $n := |G|$, $\zeta := e^{2\pi i/n}$. Nach Satz 4.10.3 ist auch $G_\zeta := \mathrm{Gal}(L(\zeta), \mathbb{Q}(\zeta))$ auflösbar. Daher besitzt G_ζ eine Normalreihe mit zyklischen Faktoren und $|G_\zeta|$ teilt $|G|$. Mit dem Hauptsatz der Galoistheorie folgt induktiv über die Anzahl der zyklischen Faktoren aus dem zyklischen Fall (Satz 4.10.2), dass die Erweiterung $L(\zeta) \mid \mathbb{Q}(\zeta)$ durch Radikale auflösbar ist. Nach Satz 4.10.3 ist dann auch $L \mid \mathbb{Q}$ durch Radikale auflösbar. □

Korollar 4.10.6. *Sei $f \in \mathbb{Q}[X]$ ein nicht-konstantes Polynom vom Grad $n \leq 4$. Dann ist die Galoisgruppe G_f von f auflösbar und f durch Radikale auflösbar.*

Beweis. Sei $L \mid \mathbb{Q}$ ein Zerfällungskörper von f über $\mathbb{Q}$. Dann ist $[L : \mathbb{Q}] \leq n! \leq 24$, siehe Satz 4.5.5, und damit $|G_f| = |\mathrm{Gal}(L, \mathbb{Q})| = [L : Q] \leq 24$. Da jede Gruppe der Ordnung ≤ 24 auflösbar ist, folgt die Behauptung. □

Bemerkung 4.10.7. Sei $f \in \mathbb{Q}[X]$ ein *irreduzibles* Polynom vom Grad $n \geq 1$. Dann ist G_f eine *transitive* Untergruppe von S_n, d.h., G_f operiert transitiv auf $\{1, 2, \ldots, n\}$. Die transitiven Untergruppen für $n \leq 4$ sind wohlbekannt. Die Fälle $n = 1, 2$ sind trivial. Für $n = 3$ sind es die Gruppen A_3, S_3, und für $n = 4$ die Gruppen $C_4, D_4, C_2 \times C_2, A_4, S_4$.

Nun können wir auch ein Beispiel eines Polynoms vom Grad 5 über $\mathbb{Q}$ geben, das *nicht* durch Radikale auflösbar ist. Es gibt also Polynomgleichungen vom Grad 5, für deren Lösung keine Wurzelformel existiert.

Beispiel 4.10.8. *Die Gleichung $X^5 - 4X + 2 = 0$ ist über $\mathbb{Q}$ nicht durch Radikale auflösbar.*

Das Polynom $f = X^5 - 4X + 2$ ist nach Eisenstein irreduzibel über $\mathbb{Q}$. Sei $L \mid \mathbb{Q}$ ein Zerfällunskörper über $\mathbb{Q}$. Wir zeigen, dass $\mathrm{Gal}(L, \mathbb{Q}) \cong S_5$ gilt. Da diese Gruppe nicht auflösbar ist nach Korollar 2.10.5, folgt die Behauptung. Die Ableitung $D(f) = 5X^4 - 4$ hat genau zwei reelle Nullstellen. Nach dem Satz von Rolle hat f also höchstens drei reelle Nullstellen. Wegen $f(-2) < 0$, $f(0) > 0$, $f(1) < 0$, $f(2) > 0$ hat f genau drei reelle Nullstellen und zwei komplex konjugierte Nullstellen, denn $f(\overline{z}) = \overline{f(z)} = \overline{0} = 0$ für eine komplexe Nullstelle $z \in \mathbb{C}$. Die komplexe Konjugation vermittelt also einen Automorphismus $\tau \in \mathrm{Gal}(L, \mathbb{Q})$ der Ordnung 2. Da $\mathrm{Gal}(L, \mathbb{Q}) \leq S_5$, können wir $\tau = (12)$ schreiben. Da f irreduzibel ist, gilt $[\mathbb{Q}(z) : \mathbb{Q}] = 5$. Wegen des Gradsatzes folgt daraus

$$5 \mid [L : \mathbb{Q}] = |\mathrm{Gal}(L, \mathbb{Q})|.$$

Aus dem Satz von Cauchy folgt, dass $\mathrm{Gal}(L, \mathbb{Q})$ ein Element σ mit $\mathrm{ord}(\sigma) = 5$ enthält. Nach Konjugation dürfen wir annehmen, dass $\sigma = (12345)$ gilt. Aber $\langle (12), (12345) \rangle = S_5$. In der Tat erzeugen (12) und $\sigma := (12 \cdots n)$ schon S_n für $n \geq 2$, weil man mit diesen beiden Elementen alle Transpositionen $(i, i+1)$ erhält, die ihrerseits S_n erzeugen:

$$\sigma^k \circ (12) \circ \sigma^{-k} = (\sigma^k(1), \sigma^k(2)) = (k+1, k+2).$$

Das Argument kann wie folgt verallgemeinert werden.

Satz 4.10.9. *Sei $f \in \mathbb{Q}[X]$ ein irreduzibles Polynom vom Grad p mit p prim. Hat f in $\mathbb{C}$ genau zwei nicht-reelle Nullstellen, dann ist die Galoisgruppe G_f von f isomorph zu S_p.*

Beweis. Sei L ein Zerfällungskörper von f über $\mathbb{Q}$ in $\mathbb{C}$ und $\alpha \in L$ eine Nullstelle von f. Da f irreduzibel ist, gilt

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = p,$$

also $p \mid [L : \mathbb{Q}] = |G_f|$. Also enthält G_f nach dem Satz von Cauchy ein Element der Ordnung p. Da p prim ist, sind die einzigen Elemente in S_p der Ordnung p durch p-Zykeln gegeben. Sei τ die komplexe Konjugation auf $\mathbb{C}$. Sie vertauscht die beiden nicht-reellen Nullstellen und fixiert die restlichen Nullstellen. Also ist $G_f \subset S_p$, und G_f enthält eine Transposition und einen p-Zykel. Diese beiden Elemente erzeugen aber in jedem Fall schon S_p. Nach Umnummerierung darf man $\tau = (12)$ annehmen. Indem man σ durch Potenzen von σ ersetzt und wieder umnummeriert, darf man zusätzlich auch $\sigma = (12 \cdots p)$ annehmen. □

Bemerkung 4.10.10. Die Galoisgruppe von f mit $\deg(f) = p$ kann auch zu S_p isomorph sein, ohne dass f genau zwei nicht-reelle Nullstellen hat. Zum Beispiel hat

$$f = X^5 - 5X^3 + 4X - 1$$

nur reelle Nullstellen und es gilt $G_f \cong S_5$.

Bemerkung 4.10.11. Sei f ein irreduzibles Polynom vom Grad 5 über $\mathbb{Q}$. Dann operiert die Galoisgruppe G_f transitiv auf den Nullstellen von f in $\mathbb{C}$ und G_f ist eine transitive Untergruppe von S_5. Es ist wohlbekannt, dass dies bis auf Konjugation die Gruppen C_5, D_5, Fr_5, A_5, S_5 sind. Hier ist $Fr_5 = \langle (12345), (1243) \rangle$ die Frobeniusgruppe der Ordnung 20. Alle genannten Gruppen können als Galoisgruppe eines Polynoms f wie oben auftreten. Die Wahl von f ist dabei allerdings nicht eindeutig. Die folgende Tabelle gibt Beispiele von solchen Polynomen, die diese Gruppen als Galoisgruppen über $\mathbb{Q}$ realisieren.

f	G_f	auflösbar
$X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$	C_5	✓
$X^5 - 5X + 12$	D_5	✓
$X^5 - 2$	Fr_5	✓
$X^5 + 20X + 16$	A_5	–
$X^5 - 4X + 2$	S_5	–

4.11 Konstruierbarkeit mit Zirkel und Lineal

Eine klassische Frage in der Geometrie ist es, welche geometrischen Objekte bzw. welche Punkte in der Ebene sich mit Zirkel und Lineal konstruieren lassen. Indem wir das Lineal durch reelle Geraden in $\mathbb{C}$ und den Zirkel durch Kreise in $\mathbb{C}$ modellieren, erhalten wir den folgenden Konstruierbarkeitsbegriff.

Definition 4.25. Sei M eine Teilmenge des Euklidischen Vektorraums $\mathbb{C} \cong \mathbb{R}^2$. Dann setzen wir

$$ZL(M) := ZL_1(M) \cup ZL_2(M) \cup ZL_3(M),$$

wobei die elementaren Konstruktionsschritte ZL_1, ZL_2, ZL_3 wie folgt definiert sind. Sei $G(M)$ die Menge aller reellen Geraden in $\mathbb{C}$, die zwei verschiedene Punkte aus M enthalten. Sei $C(M)$ die Menge aller Kreise in $\mathbb{C}$, deren Mittelpunkt in M liegt und deren Radius gleich dem Abstand zweier Punkte aus M ist. Es sei

(1) $ZL_1(M)$ die Menge aller Schnittpunkte zweier verschiedener Geraden aus $G(M)$.

(2) $ZL_2(M)$ die Menge aller Schnittpunkte von Geraden aus $G(M)$ mit Kreisen aus $C(M)$.

(3) $ZL_3(M)$ die Menge aller Schnittpunkte zweier verschiedener Kreise aus $C(M)$.

Ein Punkt $x \in \mathbb{C}$ ist aus M *mit Zirkel und Lineal konstruierbar*, wenn es ein $n \in \mathbb{N}$ mit $x \in ZL^n(M)$ gibt.

Mit dem Lineal können wir eine Gerade zwischen zwei gegebenen Punkten ziehen, und mit dem Zirkel können wir einen Kreis um den einen Punkt ziehen, der durch den anderen geht. Als Anfangsdaten haben wir zwei verschiedene Punkte in $\mathbb{C}$ oder $\mathbb{R}^2$, die ohne Einschränkung 0 und 1 sind, d.h., $(0,0)$ und $(1,0)$. Mit

$$ZL := \bigcup_{n \in \mathbb{N}} ZL^n(\{0,1\})$$

bezeichnen wir die Menge aller aus $0, 1$ mit Zirkel und Lineal konstruierbaren Punkte in $\mathbb{C}$.

Beispiel 4.11.1. *Die Konstruktion des Mittelpunktes einer Strecke zwischen zwei verschiedenen Punkten x und y, geht wie folgt.*

1. Wir zeichnen die Gerade g durch x und y.

2. Wir zeichnen den Kreis K_x um x mit Radius $r = |y - x|$ und den Kreis K_y um y mit Radius r.

3. Wir bezeichnen die beiden Schnittpunkte von K_x und K_y mit s_1 und s_2.

4. Wir zeichnen die Gerade h durch s_1 und s_2.

5. Der Schnittpunkt von g und h ist dann der gesuchte Mittelpunkt.

Satz 4.11.2 (Gauß). *Die Menge ZL in $\mathbb{C}$ ist ein Zwischenkörper von $\mathbb{C} \mid \mathbb{Q}$, der unter Quadratwurzeln abgeschlossen ist: gilt $z \in ZL$, so liegen alle Elemente $\alpha \in \mathbb{C}$ mit $\alpha^2 = z$ auch in ZL.*

Beweis. Wir schreiben $z \in \mathbb{C}$ in Polarkoordinaten, d.h., $z = e^{i\varphi} \cdot r$ mit $\varphi \in \mathbb{R}$ und $r > 0$. Dann gilt $z \in ZL$ genau dann, wenn $|z| \in ZL$ ist und der durch φ gegebene Winkel aus 0, 1 konstruierbar ist, d.h., als Winkel zwischen zwei konstruierbaren Geraden. Indem wir mit Polarkoordinaten rechnen, genügt es, die folgenden Aussagen zu zeigen.

1. Sind $x, y \in \mathbb{R} \cap ZL$, so gilt auch $x + y \in ZL$ und $x - y \in ZL$.
2. Sind φ, ψ konstruierbare Winkel, so auch $\varphi + \psi$ und $\varphi - \psi$.
3. Sind $x, y \in \mathbb{R} \cap ZL \setminus 0$, so ist $xy \in ZL$ und $\frac{1}{x} \in ZL$.
4. Ist $\varphi \in \mathbb{R}$ ein konstruierbarer Winkel, so auch $\frac{\varphi}{2}$.
5. Ist $x \in ZL$, $x > 0$, so auch $\sqrt{x} \in ZL$.

Alle Aussagen werden durch elementare geometrische Konstruktionen gezeigt. Wir überlassen $1. - 4.$ dem Leser und zeigen Punkt 5. Gegeben sei $x \in ZL$ auf der reellen Achse. Wir konstruieren auf der reellen Achse den Punkt $1 + x$ nach 1., und haben die Strecke ABC mit $A = 0$, $B = 1$, $C = x + 1$. Dann konstruieren wir den Mittelpunkt M der Strecke AC und zeichnen einen Kreis mit Zentrum M durch A und C. Nun zeichnen wir eine Gerade durch B senkrecht zu ABC. Sie schneidet den Kreis in $D = z$. Nach dem Satz von Thales sind dann 0, z und $1 + x$ die Ecken eines rechtwinkligen Dreiecks und nach dem Höhensatz gilt $x = |z - 1|^2$. Die Höhe ist $h = \sqrt{1 \cdot x}$. Mit z ist also auch h, also $\sqrt{x} = |z - 1|$ konstruierbar. □

Korollar 4.11.3. *Sind $a, b, c \in ZL$, so auch die Wurzeln der Gleichung $ax^2 + bx + c = 0$. Insbesondere ist das reguläre Pentagon konstruierbar, d.h., ζ_5 ist konstruierbar.*

Beweis. Die Wurzelformel benutzt nur Körperoperationen und Quadratwurzeln. Also sind die Wurzeln konstruierbar. Sei $\alpha = \zeta_5 + \zeta_5^4$ und $\beta = \zeta_5^2 + \zeta_5^3$. Dann gilt $\alpha\beta = \alpha + \beta = -1$. Es gilt $\alpha, \beta \in ZL$, da α, β Wurzeln der quadratischen Gleichung

$$(X - \alpha)(X - \beta) = X^2 + X - 1 = 0$$

sind. Wegen $(X - \zeta_5)(X - \zeta_5^4) = X^2 - \alpha X + 1 = 0$ ist $\zeta_5 \in ZL$. □

Theorem 4.11.4 (Charakterisierung von Konstruierbarkeit)**.** *Sei $z \in \mathbb{C}$. Die folgenden Aussagen sind äquivalent.*

(1) *Es gilt $z \in ZL$.*

(2) *Es gibt ein $n \in \mathbb{N}$ und eine Folge von Teilkörpern*

$$L_0 := \mathbb{Q} \subset L_1 \subset \cdots \subset L_n$$

in $\mathbb{C}$ mit $z \in L_n$ und $[L_j : L_{j-1}] = 2$ für alle $1 \leq j \leq n$.

(3) *Es gibt eine endliche Galoiserweiterung $L \mid \mathbb{Q}$ mit $z \in L$, deren Galoisgruppe $\mathrm{Gal}(L, \mathbb{Q})$ eine 2-Gruppe ist.*

(4) *Es gibt eine endliche Galoiserweiterung* $L \mid \mathbb{Q}$ *mit* $z \in L$ *und ein* $n \in \mathbb{N}$ *mit und* $[L : \mathbb{Q}] = 2^n$.

Beweis. (1) $\Longrightarrow$ (2): Sei $z \in ZL$, d.h., $z \in ZL^n(\{0,1\})$ für ein $n \in \mathbb{N}$. Wir beweisen 2. durch Induktion über n. Der Fall $n = 0$ ist klar wegen $ZL^0(\{0,1\}) = \{0,1\}$. Für den Induktionsschritt sei $n \geq 1$. Nach Definition von $ZL(ZL^{n-1}(\{0,1\}))$ gibt es eine endliche Menge $M \subset ZL^{n-1}(\{0,1\})$ mit $z \in ZL(M) \subset ZL(\mathbb{Q}(M))$. Nach Induktionsvoraussetzung gibt es zu jedem der Elemente aus M einen Erweiterungsturm aus Erweiterungen vom Grad 2. Durch Kombination dieser Türme folgt mit Satz 4.2.10, dass auch $\mathbb{Q}(M)$ in einem Erweiterungsturm aus Erweiterungen vom Grad 2 enthalten ist. Sei $L \subset ZL$ ein Teilkörper. Ist $x \in ZL_1(L)$, so ist $L(x) = L$. Für $x \in ZL_2(L)$ oder $x \in ZL_3(L)$ gilt offensichtlich $[L(x) : L] \leq 2$. Also hat man auch $[\mathbb{Q}(M)(z) : \mathbb{Q}(M)] \leq 2$ und durch Kombination mit dem Erweiterungsturm für $\mathbb{Q}(M)$ erhalten wir einen Erweiterungsturm für $\mathbb{Q}(z)$ bzw. z von der gewünschten Form.

(2) $\Longrightarrow$ (3): das folgt wie im Beweis von Theorem 4.10.5.

(2) $\Longrightarrow$ (1): Da ZL nach Satz 4.11.2 unter Quadratwurzeln abgeschlossen ist, gilt folgendes. Ist $L \mid \mathbb{Q}$ eine endliche Erweiterung mit $L \subset ZL$ und ist $M \subset \mathbb{C}$ mit $[M : L] = 2$, so ist $M \subset ZL$. Induktiv folgt damit die gewünschte Implikation.

(3) $\Longrightarrow$ (2): Ist $L \mid \mathbb{Q}$ eine endliche Galoiserweiterung, deren Galoisgruppe $\mathrm{Gal}(L, \mathbb{Q})$ eine 2-Gruppe ist, so folgt, dass $\mathrm{Gal}(L, \mathbb{Q})$ eine Normalreihe mit Faktoren isomorph zu C_2 besitzt. Der Hauptsatz der Galoistheorie übersetzt eine solche Normalreihe in eine Erweiterungskette wie in (2).

(3) $\Longleftrightarrow$ (4): Das ist klar wegen $[L : \mathbb{Q}] = |\mathrm{Gal}(L, \mathbb{Q})|$, siehe Satz 4.8.21. □

Korollar 4.11.5 (Quadratur des Kreises)**.** *Es ist unmöglich, mit Zirkel und Lineal aus* $0, 1$ *die Seitenlänge eines Quadrats zu konstruieren, dessen Flächeninhalt mit dem Flächeninhalt des Einheitskreises übereinstimmt.*

Beweis. Angenommen, die Quadratur des Kreises wäre möglich. Dann wäre auch $\sqrt{\pi} \in ZL$. Da π über $\mathbb{Q}$ transzendent ist, gilt das gleiche auch für $\sqrt{\pi}$. Insbesondere ist $\sqrt{\pi}$ nicht in einer endlichen Erweiterung von $\mathbb{Q}$ enthalten. Das steht jedoch im Widerspruch zu Theorem 4.11.4 oben. □

Korollar 4.11.6 (Würfelverdopplung)**.** *Es ist unmöglich, mit Zirkel und Lineal aus* $0, 1$ *die Seitenlänge eines Würfels zu konstruieren, dessen Volumen* 2 *ist.*

Beweis. Angenommen, die Würfelverdopplung wäre möglich. Dann wäre auch $\sqrt[3]{2} \in ZL$. Wegen $[\mathbb{Q}(\sqrt[3]{2}) : Q] = 3$ und der Multiplikativität des Grades folgt, dass $\sqrt[3]{2}$ nicht in einer Körpererweiterung von $\mathbb{Q}$ enthalten sein kann, deren Grad eine Zweierpotenz ist. Das ist ein Widerspruch zu Theorem 4.11.4. □

Bemerkung 4.11.7. Man kann auch leicht zeigen, dass $z \in \mathbb{C}$ genau dann konstruierbar ist, wenn der Zerfällungskörper L seines Minimalpolynoms $\mu_z \in \mathbb{Q}[X]$ den Grad $[L : Q] = 2^m$ für ein $m \in \mathbb{N}$ hat.

Korollar 4.11.8 (Reguäres n-Eck)**.** *Sei $n \geq 3$. Das reguläre n-Eck mit Radius 1 ist genau dann mit Zirkel und Lineal aus $0, 1$ konstruierbar, wenn $\varphi(n)$ eine Zweierpotenz ist.*

Beweis. Der Zerfällungskörper $\mathbb{Q}(\zeta_n)$ von Φ_n hat Grad

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n).$$

Somit ist ζ_n genau dann konstruierbar wenn $\varphi(n)$ eine Zweierpotenz ist. □

Die Folge der n für welche das regelmässige n-Eck konstruierbar ist, heißt $A003401$ in OEIS. Sie beginnt mit

$$\begin{aligned} n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, \\ 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, \\ 240, 255, 256, 257, 272, 320, 340, 384, 408, 480, 510, 512, 514, \\ 544, 640, 680, 768, 771, 816, 960, 1020, 1024, 1028, 1088, \ldots \end{aligned}$$

Bemerkung 4.11.9. Man kann auch zeigen, dass das regelmässige n-Eck genau dann konstruierbar ist, wenn n ein Produkt einer Zweierpotenz und von verschiedenen Fermat-Primzahlen $F_n = 2^{2^n} + 1$ ist. Dazu verwendet man ein elementares Lemma, welches besagt, dass eine ungerade Primzahl p mit $p - 1 = 2^m$ eine Fermat-Primzahl ist. Allerdings kennt man bis heute nur die Fermat-Primzahlen $F_0, \ldots, F_4 = 3, 5, 17, 257, 65537$. Bereits $F_5 = 1 + 2^{32} = 641 \cdot 6700417$ ist nicht prim.

Korollar 4.11.10 (Winkeldreiteilung)**.** *Im allgemeinen ist die Drittelung eines gegebenen Winkels nicht mit Zirkel und Lineal konstruierbar.*

Beweis. Angenommen, die Winkeldreiteilung wäre möglich. Dann folgte aus $e^{i\varphi} \in ZL$ auch $e^{i\varphi/3} \in ZL$. Wir zeigen, dass für $\varphi = \frac{\pi}{3}$ zwar $e^{i\varphi} \in ZL$ gilt, aber $e^{i\varphi/3} \notin ZL$. Wir wissen schon, dass $e^{i\varphi} = \zeta_6$ konstruierbar ist wegen $\varphi(6) = 2$. Nun ist $e^{i\varphi/3} = \zeta_{18}$. Wegen $\varphi(18) = 6$ ist $e^{i\varphi/3}$ nicht konstruierbar, da 6 keine Zweierpotenz ist. □

Bemerkung 4.11.11. Ist $z \in ZL$, so ist z algebraisch über $\mathbb{Q}$ mit $[\mathbb{Q}(z) : \mathbb{Q}] = 2^m$ für ein $m \in \mathbb{N}$. Die Umkehrung gilt allerdings nicht. Es gibt $z \in \mathbb{C}$, für die $[\mathbb{Q}(z) : \mathbb{Q}]$ eine Zweierpotenz ist, aber $z \notin ZL$ gilt. Zum Beispiel sind die Wurzeln z von $f = X^4 - X - 1$ wegen $G_f \cong S_4$ nicht konstruierbar, denn jede endliche Galoiserweiterung $L \mid \mathbb{Q}$ erfüllt $3 \mid [L : \mathbb{Q}]$. Trotzdem ist $[\mathbb{Q}(z) : \mathbb{Q}] = 4$, da f das Minimalpolynom von α ist.

4.12 Der Fundamentalsatz der Algebra

Den ersten Beweis des Fundamentalsatzes der Algebra erbrachte C.F. Gauß im Jahre 1799 im Rahmen seiner Dissertation. Heute sind mehrere Beweise des Fundamentalsatzes der Algebra aus unterschiedlichen Bereichen der Mathematik bekannt. Trotz

seines Namens kann der Fundamentalsatz der Algebra jedoch nicht mit rein algebraischen Methoden bewiesen werden. Dabei muss man natürlich diskutieren, was "rein algebraisch"bedeuten soll. Wir wollen hier einen Beweis mit Galoistheorie geben. Auch er verwendet unter anderem den Zwischenwertsatz aus der Analysis. Da $\mathbb{R}$ aus $\mathbb{Q}$ durch Vervollständigung hervorgeht, ist es plausibel, dass wir ohne analytische Argumente nicht auskommen. Wir fassen diese Argumente in folgendem Lemma zusammen.

Lemma 4.12.1. *1. Ist $f \in \mathbb{R}[X]$ ein Polynom ungeraden Grades, so hat f mindestens eine reelle Nullstelle.*

2. Ist $f \in \mathbb{C}[X]$ ein Polynom vom Grad 2, so zerfällt f über $\mathbb{C}$ in Linearfaktoren.

Aussage 1 kann mit dem Zwischenwertsatz bewiesen werden, Aussage 2 mit der Tatsache, dass jedes quadratische Polynom mit reellen Koefizienten eine Nullstelle in $\mathbb{C}$ hat. Nun können wir den Beweis des Fundamentalsatzes präsentieren.

Theorem 4.12.2 (Fundamentalsatz der Algebra)**.** *Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.*

Beweis. Unter Verwendung von Zerfällungskörpern genügt es zu zeigen, dass $\mathbb{C}$ keine echte endliche Erweiterung zulässt. Sei also $L \mid \mathbb{C}$ eine endliche Erweiterung. Dann ist auch $L \mid \mathbb{R}$ endlich. Wir wollen $L = \mathbb{C}$ zeigen. Sei M ein algebraischer Abschluss von L und sei $S \subset L$ eine endliche Teilmenge von M mit $L = \mathbb{R}(S)$. Indem wir die Menge $\mathcal{N}$ aller M-Nullstellen der Minmalpolynome über $\mathbb{R}$ der Elemente aus S betrachten, erhalten wir einen Körper $K := \mathbb{R}(\mathcal{N})$ mit $L \subset K$, für den die Erweiterung $L \mid \mathbb{R}$ eine endliche Galoiserweiterung ist, nach Satz 4.8.2, wobei die Separabilität in Charakteristik 0 automatisch erfüllt ist, siehe 4.8.10. Wir können daher im folgenden ohne Einschränkung annehmen, dass $L \mid \mathbb{R}$ eine endliche Galoiserweiterung mit Galosgruppe $G = Gal(L, \mathbb{R})$ ist. Wir zeigen jetzt mit 1. aus Lemma 4.12.1, dass G eine 2-Gruppe ist, und dann mit 2., dass $|G| = 2$ ist, also $L = \mathbb{C}$ gilt. Wir haben

$$[L : \mathbb{R}] = |G| = 2^k \cdot m,$$

mit $k \in \mathbb{N}$ und einer ungeraden natürlichen Zahl m. Wegen $[\mathbb{C} : \mathbb{R}] = 2$ gilt $k \geq 1$. Nach den Sylowsätzen enthält G eine 2-Sylowgruppe H. Also gilt nach 4.8.22

$$[L : L^H] = |H| = 2^k,$$

und somit

$$[L^H : \mathbb{R}] = \frac{[L : \mathbb{R}]}{[L : L^H]} = m.$$

Nach dem Satz vom primitiven Element, Theorem 4.8.17, gibt es ein $\alpha \in L$ mit $L^H = \mathbb{R}(\alpha)$. Ist $\mu_\alpha \in \mathbb{R}[X]$ das Minimalpolynom von α, so ist

$$\deg(\mu_\alpha) = [\mathbb{R}(\alpha) : \mathbb{R}] = [L^H : \mathbb{R}] = m \equiv 1 \bmod 2,$$

also nach 1. aus Lemma 4.12.1, da μ_α irreduzibel ist, $m = \deg(\mu_\alpha) = 1$ und $\alpha \in \mathbb{R}$. Nach dem Hauptsatz der Galoistheorie, Theorem 4.8.27, folgt $L^H = \mathbb{R}(\alpha) = \mathbb{R}$ und $H = G$.

Insbesondere ist G eine 2-Gruppe.

Sei $N = \mathrm{Gal}(L, \mathbb{C})$. Da $\mathbb{C} \mid \mathbb{R}$ eine Galoiserweiterung ist, folgt aus dem Hauptsatz der Galoistheorie

$$\frac{|G|}{|N|} = |G/N| = [\mathbb{C} : \mathbb{R}] = 2,$$

und N ist ebenfalls eine 2-Gruppe. Angenommen, $N \neq 1$. Dann gäbe es eine Untergruppe $U \leq N$ vom Index 2, also wäre U ein Normalteiler in N. Nach dem Hauptsatz der Galoistheorie ist dann

$$[L^U : \mathbb{C}] = |\mathrm{Gal}(L^U, \mathbb{C})| = |N/U| = 2.$$

Das steht im Widerspruch zu 2. aus Lemma 4.12.1. Also gilt $|G| = 2$ und $N = \mathrm{Gal}(L, \mathbb{C}) = 1$. Da $L \mid \mathbb{C}$ eine Galoiserweiterung ist, folgt $L = \mathbb{C}$. □

Bemerkung 4.12.3. Es gibt viele verschiedene Beweise des Fundamentalsatzes der Algebra, mit Hilfe von Algebra, Topologie, Funtionentheorie, Reeller Analysis, Riemanscher Geometrie, und anderer Gebiete. Die Frage 10535 bei *mathoverflow* hat eine Sammlung von Beweismethoden und Referenzen.

4.13 Unendliche Galoiserweiterungen

Wir haben schon unendliche Galoiserweiterungen kennengelernt, wie zum Beispiel $\overline{\mathbb{Q}} \mid \mathbb{Q}$. Die *absolute Galoisgruppe* $\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$ ist von sehr großer Bedeutung, insbesondere für die Zahlentheorie. Wir wollen nun den Hauptsatz der Galoistheorie auf unendliche Galoiserweiterungen verallgemeinern. Dazu brauchen wir aber die sogenannte *Krull Topologie* auf der Galoisgruppe.

Definition 4.26. Eine Menge G zusammen mit einer Gruppenstruktur und einer Topologie heißt *topologische Gruppe*, falls die Abbildungen

$$(g, h) \mapsto gh,\ G \times G \to G,$$
$$g \mapsto g^{-1},\ G \to G$$

beide stetig sind.

Hierbei ist $G \times G$ mit der Produkt-Topologie versehen. Es gibt zahlreiche Beispiele von topologischen Gruppen.

Beispiel 4.13.1. *1. Jede endliche Gruppe ist eine topologische Gruppe bezüglich der diskreten Topologie.*

2. Die Gruppen $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ *sind topologische Gruppen bezüglich der durch die Euklidische Metrik induzierten Topologie.*

3. Die klassischen Matrixgruppen, wie zum Beispiel

$$GL_n(\mathbb{R}),\ SL_n(\mathbb{R}),\ O_n(\mathbb{R}),\ Sp_n(\mathbb{R})$$

sind topologische Gruppen. Die Topologie auf einer solchen Gruppe G ist induziert durch die Inklusion $G \subseteq \mathbb{R}^{n^2}$.

4. Jede Lie Gruppe ist eine topologische Gruppe nach Definition. Eine Lie-Gruppe ist eine glatte reelle Mannigfaltigkeit, die zusätzlich die Struktur einer Gruppe besitzt, so dass die Gruppenverknüpfung und die Inversion beliebig oft differenzierbar sind.

Ein *Isomorphismus* von topologischen Gruppen ist ein Isomorphismus von abstrakten Gruppen und ein Homeomorphismus ihrer zugrundeliegenden topologischen Räume.

Sei G eine topologische Gruppe und $a \in G$. Dann ist die Linksmultiplikation $L_a \colon G \to G$, $g \mapsto ag$ stetig als Komposition der stetigen Abbildungen

$$G \xrightarrow{g \mapsto (a,g)} G \times G \xrightarrow{(g,h) \mapsto gh} G.$$

In der Tat ist L_a sogar ein Homeomorphismus mit inverser Abbildung $L_{a^{-1}}$. Ebenso sind die Rechtsmultiplikation R_a und die Abbildung $g \mapsto g^{-1}$ Homeomorphismen. Insbesondere gilt für jede Untergruppe H von G, dass die Nebenklasse aH von H offen ist, wenn H offen ist, und abgeschlossen, wenn H abgeschlossen ist. Das Komplement von H in G ist ja eine Vereinung solcher Nebenklassen, so dass H abgeschlossen ist, wenn es offen ist, und umgekehrt H offen ist, wenn es abgeschlossen ist und endlichen Index in G hat.

Definition 4.27. Sei X ein topologischer Raum und $x \in X$. Eine Familie $\mathcal{N}$ von Umgebungen von x heißt *Umgebungsbasis*, wenn jede offene Umgebung von x eine Menge aus $\mathcal{N}$ enthält.

Satz 4.13.2. *Sei G eine topologische Gruppe und sei $\mathcal{N}$ eine Umgebungsbasis des neutralen Elements $e \in G$. Dann gelten folgende Aussagen.*

(1) *Für alle $N_1, N_2 \in \mathcal{N}$ gibt es ein $N_3 \in \mathcal{N}$ mit $e \in N_3 \subset N_1 \cap N_2$.*

(2) *Für alle $N \in \mathcal{N}$ gibt es ein $M \in \mathcal{N}$ mit $MM \subset N$.*

(3) *Für alle $N \in \mathcal{N}$ gibt es ein $M \in \mathcal{N}$ mit $M \subset N^{-1}$.*

(4) *Für alle $N \in \mathcal{N}$ und alle $g \in G$ gibt es ein $M \in \mathcal{N}$ mit $M \subset gNg^{-1}$.*

(5) *Für alle $g \in G$ ist $\{gN \mid N \in \mathcal{N}\}$ eine Umgebungsbasis für g.*

Ist umgekehrt G eine Gruppe und $\mathcal{N}$ eine nicht-leere Menge von Teilmengen von G, die (1), (2), (3), (4) erfüllen, dann gibt es eine eindeutige Topologie auf G, für die (5) gilt.

Beweis. Sei $\mathcal{N}$ eine Umgebungsbasis von e in einer topologischen Gruppe G. Dann sind (2), (3), (4) einfach nur jeweils Konsequenzen der Stetigkeit der Abbildungen $(g,h) \mapsto gh$, $g \mapsto g^{-1}$ und $h \mapsto ghg^{-1}$. Weiterhin ist (1) eine Konsequenz der Definitionen, und (5) eine Konsequenz der Tatsache, dass L_g ein Homeomorphismus ist.

Umgekehrt sei $\mathcal{N}$ eine nicht-leere Familie von Teilmengen einer Gruppe G, die $(1)-(4)$ erfüllen. Wegen (1) liegt e in allen Mengen N von $\mathcal{N}$. Sei $\mathcal{U}$ die Familie von Teilmengen U

von G, so dass für alle $g \in U$ ein $N \in \mathcal{N}$ existiert mit $gN \subset U$. Dann gilt offensichtlich $\emptyset, G \in \mathcal{U}$ und $U_1 \cup U_2 \in \mathcal{U}$ für $U_1, U_2 \in \mathcal{U}$. Sei $g \in U_1 \cap U_2$. Nach Definition gibt es $N_1, N_2 \in \mathcal{N}$ mit $gN_1, gN_2 \in \mathcal{U}$. Aus (1) folgt, dass es ein $N_3 \in \mathcal{N}$ gibt mit $gN_3 \subset U_1 \cap U_2$. Also gilt auch $U_1 \cap U_2 \in \mathcal{U}$. Es folgt, dass die Elemente von $\mathcal{U}$ die offenen Mengen einer Topologie auf G sind, der eindeutigen Topologie auf G für die (5) gilt.

Wir wollen jetzt mit (2) und (4) zeigen, dass $(g, h) \mapsto gh$ stetig ist. Die Mengen $g_1N_1 \times g_2N_2$ bilden eine Umgebungsbasis für $(g_1, g_2) \in G \times G$. Sei $U \subset G$ eine offene Menge und (g_1, g_2) ein Paar mit $g_1g_2 \in U$. Dann müssen wir $N_1, N_2 \in \mathcal{N}$ finden mit $g_1N_1g_2N_2 \subset U$. Da U offen ist, existiert ein $N \in \mathcal{N}$ mit $g_1g_2N \subset U$. Mit (2) erhalten wir ein N_2, so dass $N_2N_2 \subseteq N$ und mit (4) ein $N_1 \in \mathcal{N}$ mit $N_1 \subset g_2N_2g_2^{-1}$. Dann haben wir

$$g_1N_1g_2N_2 \subset g_1(g_2N_2g_2^{-1})g_2N_2 = g_1g_2N_2N_2 \subset g_1g_2N \subset U.$$

Zum Schluss zeigen wir mit (3) und (4), dass auch $g \mapsto g^{-1}$ stetig ist. Sei $U \subset G$ offen und $g \in G$ mit $g^{-1} \in U$. Wir müssen ein $N \in \mathcal{N}$ finden mit $gN \subseteq U^{-1}$. Nach Definition gibt es ein $N_1 \in \mathcal{N}$ mit $g^{-1}N_1 \subset U$, also mit $N_1^{-1}g \subset U^{-1}$. Wegen (3) gibt es ein $N_2 \in \mathcal{N}$ mit $N_2 \subset N_1^{-1}$, also mit $N_2g \subset N_1^{-1}g \subset U^{-1}$, und wegen (4) gibt es ein $N \in \mathcal{N}$ mit $N \subset g^{-1}N_2g$. Dann haben wir

$$gN \subset g(g^{-1}N_2g) = N_2g \subset U^{-1}.$$

□

Definition 4.28. Sei $L \mid K$ eine nicht notwendig endliche Galoiserweiterung, d.h., eine algebraische, normale und separable Körpererweiterung. Sei $G = \mathrm{Gal}(L, K)$. Für jede endliche Teilmenge S in L sei

$$G(S) = \{\sigma \in G \mid \sigma(s) = s \text{ für alle } s \in S\}.$$

Satz 4.13.3. *Sei $L \mid K$ eine Galoiserweiterung. Dann gibt es eine eindeutig bestimmte Struktur einer topologischen Gruppe auf der Galoisgruppe*

$$G = \mathrm{Gal}(L, K),$$

für die die Mengen $G(S)$ eine Umgebungsbasis von id *bilden. Für diese Topologie bilden die Mengen $G(S)$ mit G-invariantem S eine Umgebungsbasis von* id*, die aus offenen Normalteilern besteht.*

Beweis. Wir zeigen, dass die Familie der Mengen $G(S)$ die Axiome (1) – (4) aus Satz 4.13.2 erfüllt. Offensichtlich gilt (1) wegen

$$G(S_1) \cap G(S_2) = G(S_1 \cup S_2).$$

Da jede Menge $G(S)$ eine Gruppe ist, gelten (2) und (3). Sei S eine endliche Teilmenge von L. Dann ist $K(S)$ eine endliche Erweiterung von K. Deshalb gibt es nur endlich viele

K-Homomorphismen $K(S) \to L$. Wir haben $\sigma(S) = \tau(S)$ für $\sigma_{|K(S)} = \tau_{|K(S)}$. Deshalb ist die Vereinigung

$$\overline{S} = \bigcup_{\sigma \in G} \sigma(S)$$

endlich. Weierhin ist $\sigma(\overline{S}) = \overline{S}$ für alle $\sigma \in G$. Deshalb ist $G(\overline{S})$ ein Normalteiler in G mit

$$\sigma G(\overline{S})\sigma^{-1} = G(\overline{S}) \subset G(S).$$

Somit gilt (4) und die zweite Behauptung folgt ebenfalls. □

Definition 4.29. Sei $L \mid K$ eine Galoiserweiterung mit Galoisgruppe G. Die durch $G(S)$ definierte Topologie auf G heißt *Krull Topologie*.

Wir werden in Satz 4.13.5 zeigen, dass die Krull Topologie Hausdorffsch ist. Somit ist $G = \mathrm{Gal}(L, K)$ versehen mit der Krupp Topologie eine Hausdorffsche topologische Gruppe.

Satz 4.13.4. *Sei $L \mid K$ eine Galoiserweiterung und E ein Zwischenkörper, so dass die Erweiterung $E \mid K$ endlich und Galoissch ist. Dann ist die Abbildung*

$$\mathrm{Gal}(L, K) \to \mathrm{Gal}(E, K),\ \sigma \mapsto \sigma_{|E}$$

eine stetige Surjektion, wobei $\mathrm{Gal}(E, K)$ *mit der diskreten Topologie versehen ist.*

Beweis. Sei $\sigma \in \mathrm{Gal}(E, K)$ und betrachte die Abbildung als K-Homomorphismus $E \to L$. Dann lässt sich σ zu einem L-Homomorphismus $L \to L$ fortsetzen, weswegen die Abbildung surjektiv ist. Sei S eine Menge von Erzeugern der Körpererweiterung $E \mid K$. Dann gilt $\mathrm{Gal}(E, K) = G(S)$ und deshalb ist das Urbild von $\mathrm{id}_{\mathrm{Gal}(E,K)}$ offen in G. Das gilt dann wegen *Homogenität* auch für jedes andere Element in $\mathrm{Gal}(E, K)$ und die Abbildung ist stetig. Hier bedeutet Homogenität, dass für je zwei x, y in einer topologischen Gruppe G ein Homeomorphismus $f\colon G \to G$ existiert mit $f(x) = y$. □

Satz 4.13.5. *Sei $L \mid K$ eine Galoiserweiterung. Dann ist* $\mathrm{Gal}(L, K)$ *eine kompakte, Hausdorffsche und total unzusammenhängende topologische Gruppe.*

Beweis. Sei $G = \mathrm{Gal}(L, K)$. Wir zeigen zuerst, dass G Hausdorffsch ist. Ist $\sigma \neq \tau$, dann ist $\sigma^{-1}\tau \neq \mathrm{id}_G$. Also bewegt $\sigma^{-1}\tau$ irgendein Element von L, d.h. es gibt ein $a \in L$ mit $\sigma(a) \neq \tau(a)$. Für alle S mit $a \in S$ gilt dann $\sigma G(S) \cap \tau G(S) = \emptyset$, weil ihre Elemente verschieden auf a operieren. Also sind $\sigma G(S)$ und $\tau G(S)$ zwei disjunkte offene Teilmengen von G, die σ bzw. τ enthalten. Somit ist G Hausdorffsch.

Als nächstes zeigen wir, dass G kompakt ist. Ist S eine endliche Menge, invariant unter G, dann ist $G(S)$ ein Normalteiler in G, wie wir gesehen haben. Er hat endlichen Index in G, weil er der Kern des zugehörigen Homomorphismus $G \to \mathrm{Sym}(S)$ ist. Da jede endliche Menge in einer endlichen G-invarianten Menge enthalten ist, kann man zeigen, dass die Abbildung

$$G \xrightarrow{\iota} \prod_{S \in \mathcal{S}} G/G(S)$$

injektiv ist, wobei $\mathcal{S}$ die Menge der endlichen G-invarianten Teilmengen von G bezeichnet. Wenn wir das Produkt mit der Produkt Topologie versehen, dann ist die induzierte Topologie auf G gerade die Krull Topologie, d.h. diejenige, für die die Mengen $G(S)$ eine offene Umgebungsbasis von id bilden. Der Satz von *Tychonoff* besagt nun, dass das Produkt $\prod G/G(S)$ kompakt ist. Damit bleibt nur noch zu zeigen, dass G abgeschlossen ist in dem Produkt. Für jede Inklusion $S_1 \subset S_2$ gibt es zwei stetige Abbildungen $\prod G/G(S) \to G/G(S_1)$, nämlich die kanonische Projektion π_1 auf $G/G(S_1)$ einerseits, und die kanonische Projektion π_2 auf $G/G(S_2)$ gefolgt von der Quotientenabbildung $\pi\colon G/G(S_1) \to G/G(S_2)$. Sei $E(S_1, S_2)$ die abgeschlossenen Teilmenge von $\prod G/G(S)$, auf der die beiden Abbildungen π_1 und $\pi \circ \pi_2$ übereinstimmen. Dann gilt

$$\iota(G) = \bigcap_{S_1 \subset S_2} E(S_1, E_2),$$

was abgeschlossen in $\prod G/G(S)$ ist.

Schliesslich zeigen wir, dass G total unzusammenhängend ist, d.h., dass die Zusammenhangskomponenten von G gerade die einpunktigen Mengen sind. Für jede G-invariante endliche Menge S ist $G(S)$ eine offene und damit auch abgeschlossene Untergruppe von G. Aus $\bigcap G(S) = \{\mathrm{id}\}$ folgt, dass die Zusammenhangskomponente von id in G genau $\{\mathrm{id}\}$ ist. Wegen Homogenität gilt die analoge Aussage für jedes Element in G und wir sind fertig. □

Bemerkung 4.13.6. Man kann auch zeigen, dass jede kompakte, Hausdorffsche und total unzusammenhängende topologische Gruppe als Galoisgruppe einer Galoiserweiterung in Charakteristik Null realisiert werden kann.

Satz 4.13.7. *Sei $L \mid K$ eine Galoiserweiterung. Dann gilt $L^{\mathrm{Gal}(L,K)} = K$.*

Beweis. Jedes Element von $L \setminus K$ liegt in einer endlichen Galoiserweiterung von K, so dass die Aussage aus der Surjektivität in Satz 4.13.4 folgt. □

Wir kommen nun zum Hauptsatz der unendlichen Galoiserweiterungen. Bereits Dedekind bemerkte, dass der Hauptsatz für endliche Galoiserweiterungen nicht mehr gelten muss für unendliche Galoiserweiterungen. Dazu sei $K = \mathbb{F}_p$ und

$$\mathbb{F} := \bigcup_{n \geq 1} \mathbb{F}_{p^n}$$

ein algebraischer Abschluss von $\mathbb{F}_p$. Sei $L = \mathbb{F}$. Die Erweiterung $\mathbb{F} \mid \mathbb{F}_p$ ist Galoissch mit Galoisgruppe $G = \mathrm{Gal}(L, K)$. Sei H die Untergruppe von G, die von dem Frobeniusautomorphismus $\varphi\colon \alpha \to \alpha^p$ erzeugt wird.

Satz 4.13.8. *Es gilt $L^H = L^G = K$ mit $H \neq G$. Also gibt es zwei verschiedene Untergruppen von G mit dem gleichen Fixkörper, d.h., der Hauptsatz gilt nicht für die Galoiserweiterung $\overline{\mathbb{F}_p} \mid \mathbb{F}_p$.*

Beweis. Offensichtlich gilt $L^G = K$, mit $L = \mathbb{F}$ und $K = \mathbb{F}_p$. Sei $x \in L^H$. Dann ist $\varphi(x) = x$, also ist x eine Nullstelle von $X^p - X \in K[X]$. Alle Elemente von K sind Nullstelle dieses Polynoms. Da K ein Körper ist, kann es nicht mehr als p Nullstellen geben. Also ist $x \in K$ und es gilt $L^H = K$. Nun wollen wir zeigen, dass H eine echte Untergruppe von G ist. Dazu genügt es, ein $\tau \in \mathrm{Gal}(L, K)$ zu konstruieren, dass keine Potenz von φ ist. Das erreichen wir mit der Konstruktion eines *unendlichen* Zwischenkörpers M mit

$$K \subsetneqq M \subsetneqq L.$$

Man wähle ein $\tau \in \mathrm{Gal}(L, M)$ mit $\tau \neq \mathrm{id}$. Das macht Sinn, weil auch $L \mid M$ Galoissch ist. Angenommen, es wäre $H = G$. Dann hätten wir $\tau = \varphi^n$ für ein $n \geq 1$. Wir können τ durch τ^{-1} ersetzen, falls nötig. Dann stabilisiert φ^n den Körper M elementweise und M ist im Fixkörper von φ^n enthalten, d.h. $M \subset \mathbb{F}_{p^n}$. Das ist aber ein Widerspruch, da M unendlich ist. Also gilt $H \neq G$.

Um den Beweis zu vollenden, müssen wir also einen solchen unendlichen Körper M finden. Eine mögliche Wahl ist durch

$$M := \bigcup_{n \geq 0} \mathbb{F}_{p^{2^n}}$$

gegeben. Offensichtlich ist M unendlich und in L enthalten. Wir zeigen, dass $M \neq L$ gilt. Sei C eine kubische Körpererweiterung von $K = \mathbb{F}_p$, also mit $[C : \mathbb{F}_p] = 3$. Deshalb gibt es ein $\alpha \in L$ mit $C = \mathbb{F}_p(\alpha)$. Angenommen es gilt $\alpha \in M$. Dann gilt $\alpha \in \mathbb{F}_{p^{2^n}}$ für ein n und

$$2^n = [\mathbb{F}_{p^{2^n}} : \mathbb{F}_p] = [\mathbb{F}_{p^{2^n}} : C] \cdot [C : \mathbb{F}_p].$$

das ist ein Widerspruch zu $3 \nmid 2^n$, und wir sind fertig. □

Wie muss man den Haupsatz für unendliche Galoiserweiterungen modifizieren, damit die Aussage gültig bleibt? Die Antwort liegt in der Krull Topologie. Für eine Untergruppe H einer topologischen Gruppe G bezeichne $\overline{H}$ den Abschluss von H in G. In unserem Beispiel aus Satz 4.13.8 gilt dann $G = \overline{H}$ wenn wir den Abschluss betrachten, und die Eindeutigkeit ist wiederhergestellt.

Satz 4.13.9. *Sei $L \mid K$ eine Galoiserweiterung mit Galoisgruppe $G = \mathrm{Gal}(L, K)$. Dann ist auch $L \mid M$ eine Galoiserweiterung für jeden Unterkörper M, der K enthält und $\mathrm{Gal}(L, M)$ ist abgeschlossen in G mit*

$$L^{\mathrm{Gal}(L,M)} = M.$$

Für jede Untergruppe H von G gilt $\mathrm{Gal}(L, L^H) = \overline{H}$.

Beweis. Für jede endliche Menge $S \subset M$ ist $G(S)$ eine offene Untergruppe von G, also auch abgeschlossen. Wegen

$$\mathrm{Gal}(L, M) = \bigcap_{S \subset M} G(S)$$

ist die Galoisgruppe also auch offen, und demnach abgeschlossen. Wegen Satz 4.13.7 gilt $L^{\mathrm{Gal}(L,M)} = M$.

Da $\mathrm{Gal}(L, L^H)$ abgeschlossen ist und H enthält, gilt $\overline{H} \subset \mathrm{Gal}(L, L^H)$. Umgekehrt sei $\sigma \in G \setminus \overline{H}$. Dann ist $\sigma(G(S)) \cap H = \emptyset$ für eine endliche Teilmenge S von L, von der wir OBDA annehmen dürfen, das sie G-invariant ist. Also ist $\sigma \notin H \cdot G(S)$ und es gibt ein $\alpha \in K(S)$, das festbleibt unter H, aber nicht unter σ. Das zeigt $\sigma \notin \mathrm{Gal}(L, L^H)$ und somit $\mathrm{Gal}(L, L^H) = \overline{H}$. □

Analog zum Hauptsatz der Galoistheorie, Theorem 4.8.27, erhalten wir nun den Hauptsatz der unendlichen Galoistheorie. Es bezeichne $\mathcal{U}(G)$ die Menge aller *abgeschlossenen* Untergruppen einer Gruppe G und $\mathcal{Z}(L \mid K)$ die Menge aller Zwischenkörper einer Erweiterung $L \mid K$.

Theorem 4.13.10 (Hauptsatz der unendlichen Galoistheorie)**.** *Sei $L \mid K$ eine Galoiserweiterung mit Galoisgruppe $G = \mathrm{Gal}(L, K)$. Dann sind die Abbildungen*

$$\mathcal{Z}(L, K) \to \mathcal{U}(G), \quad M \mapsto \mathrm{Gal}(L, M)$$
$$\mathcal{U}(G) \to \mathcal{Z}(L \mid K), \quad H \mapsto L^H$$

zueinander inverse Bijektionen. Es gelten folgende Aussagen.

(1) *Die Korrespondenz ist inklusionsumkehrend, d.h., es gilt*

$$H_1 \supset H_2 \iff L^{H_1} \subset L^{H_2}.$$

(2) *Eine abgeschlossene Untergruppe H von G ist genau dann offen, wenn L^H endlichen Grad über K hat. Dann gilt $(G : H) = [L^H : K]$.*

(3) *Die Untergruppe $\sigma H \sigma^{-1}$ korrespondiert zu dem Zwischenkörper $\sigma(M)$, d.h., es gilt $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$ und $\mathrm{Gal}(L, \sigma(M)) = \sigma\,\mathrm{Gal}(L \mid M)\sigma^{-1}$.*

(4) *Eine abgeschlossene Untergruppe H von G ist genau dann Normalteiler in G wenn $L^H \mid K$ Galoissch ist. Dann gilt $\mathrm{Gal}(L^H, K) \cong G/H$.*

Beweis. Die Aussagen sind klar bis auf einige topologische Argumente. Für (2) beachte man, dass jede abgeschlossene Untergruppe von endlichem Index in einer topologischen Gruppe auch offen ist. Da G kompakt ist, ist umgekehrt auch jede offene Untergruppe von G immer von endlichem Index. Sei H eine solche Untergruppe von G. Dann induziert die Abbildung $\sigma \mapsto \sigma_{|L^H}$ eine Bijektion $G/H \to \mathrm{Hom}_K(L^H, L)$ und es folgt $(G : H) = [L^H : K]$. Zu (4) sei M in Korrespondez zu H. Aus (3) folgt, dass H genau dann Normalteiler ist, wenn M invariant unter der G-Aktion ist. Aber das gilt genau dann, wenn M eine Vereinigung von endlichen Erweiterungen von K ist, invariant unter G, d.h. eine Vereinigung von endlichen Galoiserweiterungen. Aber eine Erweiterung ist Galoissch genau dann, wenn sie eine Vereinigung von endlichen Galoiserweiterungen ist. □

Bemerkung 4.13.11. Sei $(M_i)_{i\in I}$ eine Familie von Zwischenkörpern und H_i die zugehörige Unetrgruppe zu M_i. Sei $\prod_i M_i$ der kleinste Körper, der alle M_i enthält. Da $\bigcap_{i\in I} H_i$ die größte abgeschlossene Untergruppe von G ist, die alle H_i enthält, folgt

$$\mathrm{Gal}(M, \prod_i M_i) = \bigcap_{i\in I} H_i.$$

Satz 4.13.12. *Seien E und L Körpererweiterungen von K. Ist $E \mid K$ Galoissch, dann sind auch $EL \mid L$ und $E \mid E\cap L$ Galoissch und die Abbildung*

$$\sigma \mapsto \sigma_{|E},\ \mathrm{Gal}(EL, L) \to \mathrm{Gal}(E, E\cap L)$$

ist ein Isomorphismus topologischer Gruppen.

Beweis. Wir müssen nur noch die topologischen Argumente geben. Dazu zeigen wir, dass die Abbildung auch stetig und offen ist. Seien also $G_1 = \mathrm{Gal}(EL, L)$ und $G_2 = \mathrm{Gal}(E, E\cap L)$. Für jede endliche Menge S von Elementen aus E ist das Urbild von $G_2(S)$ in G_1 durch $G_1(S)$ gegeben. Also ist die Abbildung stetig. Eine offene Untergruppe von $\mathrm{Gal}(EL, L)$ ist abgeschlossen, also auch kompakt, von endlichem Index. Also ist auch ihr Bild in $\mathrm{Gal}(E, E\cap L)$ kompakt, also abgeschlossen von endlichem Index, also offen. □

Wir wollen noch einmal auf Satz 4.13.8 zurückkommen, in dem wir die Galoiserweiterung $\overline{\mathbb{F}_p} \mid \mathbb{F}_p$ studiert haben. Wie können wir ihre Galoisgruppe beschreiben? Man betrachte die additive Gruppe $\mathbb{Z}$ und versehe sie mit der Topologie, für die die Gruppen $n\mathbb{Z}$ für $n \geq 1$ eine offene Umgebungsbasis von 0 bilden. Zwei ganze Zahlen sind darin also nahe beieinander, wenn ihre Differenz durch eine große ganze Zahl teilbar ist. In diesem Sinne ist $\mathbb{Z}$ eine topologische Gruppe, die wir vervollständigen können. Eine *Cauchyfolge* in $\mathbb{Z}$ sei eine Folge $(a_i)_{i\in I}$ mit $a_i \in \mathbb{Z}$, für die gilt: für alle $n \geq 1$ gibt es ein N mit $a_i \equiv a_j \bmod n$ für alle $i, j > N$. Eine solche Cauchyfolge heißt *trivial*, falls $a_i \to 0$ for $i \to \infty$, d.h., wenn für alle $n \geq 1$ ein N existiert mit $a_i \equiv 0 \bmod n$ für alle $i > N$. Die Cauchyfolgen bilden eine kommutative Gruppe C und die trivialen Cauchyfolgen eine Untergruppe T. Wir definieren die Quotientengruppe als

$$\widehat{\mathbb{Z}} = C/T.$$

Das hat auch eine Ringstruktur, und wir können $\mathbb{Z}$ als Untergruppe von $\widehat{\mathbb{Z}}$ auffassen mit der Abbildung $m \mapsto (m, m, m, \cdots)$. Man beachte, dass die Gruppe überabzählbar und total unzusammenhängend ist. Sei $\mathbb{Z}_p$ der Ring der p-adischen ganzen Zahlen. Wir haben folgendes Resultat.

Satz 4.13.13. *Sei $\mathbb{F}$ ein algebraischer Abschluss von $\mathbb{F}_p$. Dann ist die Galoisgruppe von $\mathbb{F} \mid \mathbb{F}_p$ gegeben durch*

$$\mathrm{Gal}(\mathbb{F}, \mathbb{F}_p) \cong \widehat{\mathbb{Z}} \cong \prod_{p\in\mathbb{P}} \mathbb{Z}_p.$$

Beweis. Sei $\alpha \in \widehat{\mathbb{Z}}$ durch die Cauchyfolge (a_i) representiert, $G = \mathrm{Gal}(\mathbb{F}, \mathbb{F}_p)$ und $\sigma \in G$. Dann hat die Einschränkung $\widetilde{\sigma}$ von σ auf $\mathbb{F}_{p^n}$ die Ordnung n. Also ist $\widetilde{\sigma}^{a_i}$ unabhängig von i für genügend großes i und wir können σ^α durch

$$\sigma^\alpha | \mathbb{F}_{p^n} = \widetilde{\sigma}^{a_i}$$

für alle n und alle $i \geq n_0$, abhängig von n, definieren. Damit erhalten wir eine Abbildung

$$\widehat{\mathbb{Z}} \to \mathrm{Gal}(\mathbb{F}, \mathbb{F}_p),\ \alpha \mapsto \sigma^\alpha,$$

die offentlichtlich ein Isomorphismus ist. □

Galoisgruppen sind die Motivation für uns, abschliessend kurz auf sogenannte *proendliche* Gruppen einzugehen.

Definition 4.30. Eine partiell geordnete Menge $(I, \leq)$ heißt *gerichtet* falls es für je zwei Elemente $i, j \in I$ ein $k \in I$ gibt mit $i, j \leq k$. Es gebe für jedes Element i einer gerichteten Menge $(I, \leq)$ eine Gruppe G_i und für jede Ungleichung $i \leq j$ einen Gruppenhomomorphismus $\pi_{ji} \colon G_j \to G_i$ mit

(1) $\pi_{ii} = \mathrm{id}$ für alle $i \in I$,

(2) $\pi_{ji} \circ \pi_{kj} = \pi_{ki}$ für alle $i \leq j \leq k$.

Dann heißt die Familie (G_i, π_{ji}) ein *projektives System* von Gruppen (einige Autoren schreiben $(I, \leq, G_i, \pi_{ji})$). Für ein solches projektives System definiert man den *projektiven Limes* durch

$$\varprojlim G_i = \{(g_i)_{i \in I} \in \prod_{i \in I} G_i \mid \pi_{ji}(g_j) = g_i \text{ wann immer } i \leq j\}.$$

Dieser Limes ist in der Tat eine Gruppe, nämlich eine Untergruppe des direkten Produkts $\prod G_i$. Das neutrale Element ist $(1, 1, 1, \ldots)$. Es liegt in $\varprojlim G_i$. Sind $g, h \in \varprojlim G_i$ mit $g = (\cdots, g_i, \cdots)$ und $h = (\cdots, h_i, \cdots)$ dann ist auch $gh = (\cdots, g_i h_i, \cdots) \in \varprojlim G_i$. In der Tat,

$$\pi_{ji}(g_j h_j) = \pi_{ji}(g_j)\pi_{ji}(h_j) = g_i h_i.$$

Die Gruppe $\varprojlim G_i$ ist mit Projektionen $\varprojlim G_i \to G_j$ ausgestattet, die durch die Projektionen $\pi_j \colon \prod G_i \to G_j$ induziert sind. Außerdem ist $\varprojlim G_i$ auch eine topologische Gruppe. Jedes G_i ist mit der diskreten Topologie versehen, das Produkt $\prod G_i$ mit der Produkt Topologie und der projektive Limes mit der Einschränkungstopologie.

Satz 4.13.14. *Sei (G_i, π_{ji}) ein projektives System von Gruppen, wobei alle G_i kompakte Hausdorffsche topologische Gruppen sind. Dann ist auch $\varprojlim G_i$ eine kompakte Hausdorffsche topologische Gruppe.*

Beweis. Nach dem Satz von Tychonoff ist das Produkt $\prod G_i$ zusammen mit der Produkt Topologie kompakt, weil alle G_i kompakt sind. Die Produkt Topologie ist die gröbste Topologie, in der alle Projektionen $\pi_j \colon \prod G_i \to G_j$ stetig sind. Es genügt zu zeigen, dass $\varprojlim G_i$ abgeschlossen ist in $\prod G_i$ bezüglich der Relativtopologie, denn daraus folgt, dass $\varprojlim G_i$ eine kompakte topologische Gruppe ist. Sei $g = (\ldots, g_i, \ldots)$ in $\prod G_i \setminus \varprojlim G_i$. Dann gibt es ein Indexpaar (i, j) mit $j \geq i$ und $\pi_{ji}(g_j) \neq g_i$. Da alle G_i Hausdorffsch sind, gibt es offene Umgebungen V_j von $\pi_{ji}(g_j) \in G_i$ und U_i von $g_i \in G_i$ mit $V_j \cap U_i = \emptyset$. Da π_{ji} stetig ist, ist $U_j = \pi_{ji}^{-1}(V_j)$ eine offene Umgebung von $g_j \in G_j$. Dann ist

$$U = U_i \times U_j \times \prod_{k \neq i,j} G_k$$

eine offene Umgebung von $g \in G$, die disjunkt mit $\varprojlim G_i$ ist. In der Tat ist $U \cap \varprojlim G_i = \emptyset$, weil $\pi_{ji}(U_j) \subset V_j$ und U_i einen leeren Schnitt haben. Also ist $\prod G_i \setminus \varprojlim G_i$ offen, weil jedes $g \in \prod G_i \setminus \varprojlim G_i$ eine offene Umgebung hat, die $\varprojlim G_i$ nicht schneidet. Also ist $\varprojlim G_i$ abgeschlossen. □

Definition 4.31. Eine topologische Gruppe die isomorph zu einem projektiven Limes endlicher Gruppe ist heißt *pro-endliche Gruppe*.

Die Definition eines pro-endlichen Ringes ist analog. Tatsächlich haben wir solche Gruppen schon kennengelernt, als Galoisgruppen von unendlichen Galoiserweiterungen. Das folgende Resultat ist leicht zu zeigen.

Satz 4.13.15. *Sei G eine topologische Gruppe. Dann sind die folgenden Aussagen äquivalent.*

(1) G ist eine pro-endliche Gruppe.

(2) G ist eine kompakte, Hausdorffsche, und total unzusammenhängende Gruppe.

Beispiel 4.13.16. *Jede endliche Gruppe G ist pro-endlich.*

In der Tat, sei $I = \{1\}$, $G_i = G$ und $\pi_{11} = \mathrm{id}$. Man versehe die endlichen Gruppen G_i mit der diskreten Topologie. Dann ist (G_i, π_{ji}) ein projektives System mit Limes G. Also ist G pro-endlich. Umgekehrt ist jede diskrete pro-endliche Gruppe endlich.

Beispiel 4.13.17. *Die Gruppe $\mathbb{Z}$ ist nicht pro-endlich. Ihre pro-endliche Vervollständigung $\widehat{\mathbb{Z}}$ ist pro-endlich.*

In der Tat, $\mathbb{Z}$ ist nicht kompakt. Für die pro-endliche Vervollständigung siehe Definition 4.32. Sie stimmt mit der Definition vor Satz 4.13.13 überein.

Beispiel 4.13.18. *Die p-adischen ganzen Zahlen $\mathbb{Z}_p$ bilden einen pro-endlichen Ring.*

Dazu seien $R_i = \mathbb{Z}/p^i\mathbb{Z}$ und $\pi_{ji} \colon \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ die natürliche Projektionen. Der projektive Limes dieser Ringe ist wieder ein Ring. Es ist der *Ring der p-adischen ganzen Zahlen*

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^i\mathbb{Z}.$$

Wir können die Elemente wie folgt beschreiben:

$$\mathbb{Z}_p = \{(x_n)_{n=0}^{\infty} \in \prod_{n\geq 0} \mathbb{Z}/p^n\mathbb{Z} \mid x_{n+1} \equiv x_n \mod p^n\}.$$

Definition 4.32. Sei G eine Gruppe. Die *pro-endliche Vervollständigung* von G ist die pro-endliche Gruppe $\widehat{G}$, die durch $\widehat{G} = \varprojlim G/N$ definiert wird, wobei N die Normalteiler von endlichem Index in G durchläuft, nach Inklusion geordnet, und zusammen mit den natürlichen Abbildungen π_{ji}.

Man hat den natürlichen Gruppenhomomorphismus $G \to \widehat{G}$ mit dichtem Bild, der aber im allgemeinen nicht injektiv sein muß.

Beispiel 4.13.19. *Die pro-endliche Vervollständigung der Gruppe $\mathbb{Z}$ ist gegeben durch*

$$\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} \cong \prod_{p\in\mathbb{P}} \mathbb{Z}_p.$$

Das ist die Galoisgruppe von $\overline{\mathbb{F}_p} \mid \mathbb{F}_p$, siehe Satz 4.13.13.

Dazu sei I die Menge der positiven ganzen Zahlen, partiell geordnet durch

$$n \leq m \Longleftrightarrow n \mid m.$$

Dann ist $(I, \leq)$ gerichtet und $(I, \leq, \mathbb{Z}/nZ, \pi_{mn})$ ist ein projektives System mit projektivem Limes $\widehat{\mathbb{Z}}$. Die π_{mn} sind wiederum die üblichen Surjektionen.

Beispiel 4.13.20. *Sei L/K eine Galoiserweiterung. Dann ist $Gal(L/K)$ eine pro-endliche Gruppe und die pro-endliche Topologie stimmt auf ihr mit der Krull Topologie überein.*

Sei $\mathcal{Z}$ die Menge der Zwischenkörper F_i in der Erweiterung $L \mid K$, so dass $F_i \mid K$ eine endliche Galoiserweiterung ist. Die Menge $\mathcal{Z}$ ist partiell geordnet durch Inklusion. Wir können das Kompositum zweier Zwischenkörper nehmen, das wiederum eine endliche Galoiserweiterung ist. Also ist die Menge $\mathcal{Z}$ gerichtet. Für $F_j \supset F_i$ haben wir die Einschränkungsabbildungen

$$\pi_{ji} \colon Gal(F_j/K) \to Gal(F_i/K).$$

Damit haben wir ein projektives System mit

$$Gal(L/K) = \varprojlim Gal(F_i/K),$$

wobei nun jede Gruppe $Gal(F_i/K)$ endlich ist. Damit haben wir $Gal(L/K)$ mit der pro-endlichen Topologie versehen. Sie stimmt mit der Krull Topologie überein. Das folgt auch aus folgendem Lemma.

Lemma 4.13.21. *Sei $(I, \leq, G_i, \pi_{ij})$ ein projektives System endlicher Gruppen und $G = \varprojlim G_i$ die zugehörige pro-endliche Gruppe. Seien $\pi_i \colon G \to G_i$ die Projektionen, die von den Projektionen $\prod G_j \to G_i$ induziert sind. Dann bilden die Mengen $\{\ker(\pi_i) \mid i \in I\}$ eine offene Umgebungsbasis von* id *in G.*

Beweis. Da alle G_i endlich sind, versehen mit der diskreten Topologie, ist $\{\mathrm{id}\}$ eine offene Umgebungsbasis von id in G_i. Nach Definition der Produkt Topologie von $\prod G_i$ und der Relativtopologie von $G \subseteq \prod G_i$ bilden die Mengen

$$G \cap \left(\prod_{j \in J} \{1\} \times \prod_{i \in I \setminus J} G_i \right) = \bigcap_{J \subseteq I} \ker(\pi_i)$$

eine offene Umgebungsbasis von id in G, wobei J die *endlichen* Teilmengen von I durchläuft. Da I gerichtet ist und alle J endlich sind, existiert ein $k \in I$ mit $j \leq k$ für alle $j \in J$. Daraus folgt

$$\ker(\pi_k) \subseteq \bigcap_{J \subseteq I} \ker(\pi_i),$$

so dass die Kerne der Projektionen π_i eine offene Umgebungsbasis von id in G bilden. □

Wir identifizieren also nun die pro-endliche Topologie und die Krull Topologie auf $G = Gal(L/K)$. Eine offene Umgebungsbasis von id in der Krull Topologie auf $G = Gal(L/K)$ besteht aus den Gruppen $G_i = Gal(L/F_i)$, wobei $F_i \mid K$ endlich und normal ist. Es gilt $G = \varprojlim G_i$ und $\ker(\pi_i) = Gal(L/F_i)$, da $\ker(\pi_i)$ aus allen Körperautomorphismen von L besteht, die trivial auf F_i sind.

Bemerkung 4.13.22. Natürlich folgt auch schon aus Satz 4.13.5 und Satz 4.13.15, dass $Gal(L/K)$ eine pro-endliche Gruppe ist.

Wir erwähnen einige Eigenschaften von pro-endlichen Gruppen.

Satz 4.13.23. *Sei H eine abgeschlossene Untergruppe einer pro-endlichen Gruppe G. Dann ist auch H pro-endlich.*

Man beachte, dass die Abgeschlossenheit hier notwendig ist. Wir haben bereits die pro-endliche Gruppe $Gal(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ betrachtet, mit ihrer Untergruppe H, die durch den Frobeniusautomorphismus erzeugt wird. Es ist $H \simeq \mathbb{Z}$, was keine pro-endliche Gruppe ist (nicht kompakt).

Satz 4.13.24. *Sei N ein abgeschlossener Normalteiler der pro-endlichen Gruppe G. Dann ist G/N pro-endlich bezüglich der Quotiententopologie.*

Wir haben schon erwähnt, dass offene Untergruppen H von G einen endlichen Index haben. In der Tat ist G kompakt und $\bigcup_{g \in G} gH$ eine offene Überdeckung von G. Andererseits müssen Untergruppen von endlichem Index in pro-endlichen Gruppen nicht notwendig offen sein. Wir werden zeigen, dass $\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$ nicht-offene Normalteiler vom Index 2^n hat, für jedes $n \geq 1$. Dazu zeigen wir zuerst das folgende Lemma.

Lemma 4.13.25. *Sei V ein unendlich-dimensionaler Vektorraum. Dann existiert für alle $n \geq 1$ ein Unterraum V_n von V, so dass V/V_n die Dimension n hat.*

Beweis. Aus Zorns Lemma folgt, dass V maximal linear unabhängige Teilmengen besitzt, die eine Basis von V bilden. Man wähle eine solche Basis und lasse exakt n Elemente davon weg. Der davon erzeugte Unterraum sei V_n. □

Satz 4.13.26. *Die pro-endliche Gruppe $Gal(\overline{\mathbb{Q}}, \mathbb{Q})$ hat nicht-offene Normalteiler von endlichem Index 2^n für jedes $n \geq 1$.*

Beweis. Sei E der Unterkörper

$$\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \ldots]$$

des Körpers $\mathbb{C}$. Für jede Primzahl $p \in \mathbb{P}$ gilt

$$Gal(\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \ldots, \sqrt{p}], \mathbb{Q}) \simeq \prod_{\substack{\ell \in \mathbb{P}, \ell \leq p \\ \ell = \infty}} \mathbb{Z}/2\mathbb{Z}.$$

Deshalb ist

$$G := Gal(E, \mathbb{Q}) = \varprojlim_n Gal(\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \ldots, \sqrt{p}], \mathbb{Q})$$

ein direktes Produkt von Kopien von $\mathbb{Z}/2\mathbb{Z}$, indiziert durch die Primzahlen ℓ von $\mathbb{Q}$ einschließlich $\ell = \infty$. Man beachte die folgende Untergruppe H von G:

$$H = \{(a_\ell) \in G \mid a_\ell = 0 \text{ für fast alle } \ell\}.$$

Diese Untergruppe ist dicht in G, weil es für jeden Punkt $(a_\ell) \in G$ eine Folge in H gibt, die gegen (a_ℓ) konvergiert, gegeben durch

$$(a_\infty, 0, 0, 0, \ldots),\ (a_\infty, a_2, 0, 0, \ldots),\ (a_\infty, a_2, a_3, 0, \ldots),\ \ldots$$

Wir können G/H als Vektorraum über $\mathbb{F}_2$ ansehen. Wegen Lemma 4.13.25 existiert eine Untergruppe G_n vom Index 2^n in G, die H enthält. G_n kann nicht offen sein, weil sie sonst auch abgeschlossen wäre, im Widerspruch dazu, dass sie dicht ist. Also ist das Urbild von G_n in $Gal(\overline{\mathbb{Q}}, \mathbb{Q})$ ein nicht-offener Normalteiler von endlichem Index. □

Eine pro-endliche Gruppe heißt *topologisch endlich-erzeugt*, falls sie eine dichte, endlich erzeugte Untergruppe hat.

Theorem 4.13.27 (Nikolov, Segal 2003)**.** *Sei G eine topologisch endlich-erzeugte pro-endliche Gruppe. Dann sind alle Untergruppen von endlichem Index offen.*

Diese Ergebnis verallgemeinert ein früheres analoges Resultat von Jean-Pierre Serre für topologisch endlich-erzeugte pro-p-Gruppen. Der Beweis benutzt die Klassifikation endlicher einfacher Gruppen.

Der folgende Satz ist in [6] bewiesen, Theorem 2.11.5.

Satz 4.13.28. *Jede pro-endliche Gruppe kann als Galoisgruppe einer entspechenden Galoiserweiterung realisiert werden.*

Bemerkung 4.13.29. Im Gegensatz dazu kann *nicht* jede pro-endliche Gruppe als absolute Galoisgruppe realisiert werden.

In der Tat, es folgt aus dem Satz von Artin-Schreier, dass die einzigen *endlichen* absoluten Galoisgruppen durch $Gal(\mathbb{C}/\mathbb{C}) = 1$ und $Gal(\mathbb{C}/\mathbb{R}) = C_2$ gegeben sind.

Theorem 4.13.30 (Artin-Schreier, 1927)**.** *Sei K ein algebraisch abgeschlossener Körper und F ein Unterkörper mit $1 < [K : F] < \infty$. Dann ist $K \mid F$ eine Galoiserweiterung, $K = F(i)$ mit $i^2 = -1$, und F hat Charakteristik Null. Weiterhin ist jede endliche Summe von nicht-verschwindenden Quadraten wieder ein nicht-verschwindendes Quadrat in F.*

Literaturverzeichnis

[1] H. U. Besche, B. Eick, E. A. O'Brien: *A millennium project: constructing small groups.* Internat. J. Algebra Comput. **12** (2002), no. 5, 623–644.

[2] M. Harper: $\mathbb{Z}[\sqrt{14}]$ *is Euclidean.* Canad. J. Math. **56** (2004), 55–70.

[3] G. Higman: *Enumerating p-groups. I: Inequalities.* Proc. London Math. Soc. (3) **10** (1960), 24–30.

[4] J. C. Jantzen, J. Schwermer: *Algebra.* Springer-Verlag (2006).

[5] G. Mackiw: *Finite Groups of* 2×2 *Integer Matrices.* Math. Magazine **69**, No. 5 (1996), 356–361.

[6] L. Ribes, P. Zalesskij: *Profinite groups.* Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 40, Springer Verlag **2000**.

[7] H. M. Stark: *A complete determination of the complex quadratic fields of class-number one.* Michigan Math. Journal **14** (1967), 1–27.

[8] T. Szele: *Über die endichen Ordnungszahlen, zu denen nur eine Gruppe gehört.* Comment. Math. Helv. **20**, (1947). 265–267.